REVISTA DE DERECHO PENAL Y CRIMINOLOGÍA, 3.ª Época, n.º 3 (2010), págs. 73-134

SUPLANTACIÓN DE IDENTIDAD Y USO DE NOMBRE SUPUESTO EN EL COMERCIO TRADICIONAL Y ELECTRÓNICO[1]

PATRICIA FARALDO CABANA
Profesora Titular de Derecho penal
Universidad de A Coruña

Resumen: En este trabajo se analiza el fenómeno delictivo de la suplantación de identidad y uso de nombre supuesto tanto en el comercio tradicional como en el electrónico, que da lugar a soluciones dispares en la doctrina y jurisprudencia. Se presentan las posibilidades que ofrecen los delitos de usurpación de estado civil, estafa, falsedad documental y falsificación de moneda para abarcar las conductas relacionadas con la presentación al pago de tarjetas ajenas sin autorización del titular y con la falsificación y posterior uso de tarjetas. Para ello se parte de un análisis de los mecanismos de identidad en la sociedad de la información y de cómo sus puntos débiles son aprovechados por los delincuentes para la comisión de delitos.

Palabras clave: suplantación de identidad, estaf, falsificación de tarjetas, comercio electrónico.

Abstract: This paper analyses the crime of phishing and of using false names in the traditional and the e-commerce. Such phenomena have led to disparate solutions in both the academic and the sentencing fields. The unauthorised use and the falsification and later use of credits cards are regarded as encompassed by different felonies such as the encroachment of the marital status, fraud, forgery or currency diddling. To fulfil the mentioned objectives, a study of the identity

[1] Este trabajo se enmarca en el Proyecto de Investigación «Espacio y Derecho Penal» (DER2008-01523/JURI), financiado por el Ministerio de Ciencia e Innovación.

mechanisms of the information society and how offenders take advantage of its weaknesses is carried out.

Keywords: identity fraud, fraud, card fraud, e-commerce.

I. Introducción

Con las expresiones suplantación, usurpación o robo de identidad[2] se pretende en este trabajo aludir al comportamiento delictivo consistente en que el autor utiliza los datos relativos a la identidad de otra persona para hacerse pasar por ella en el tráfico jurídico-económico[3], datos que a veces se obtienen de forma fraudulenta y a veces en connivencia con el titular legítimo, en ocasiones para causar un perjuicio, patrimonial o de otro tipo, al titular o a otra persona, y en otras con finalidades distintas. Por su parte, el uso de nombre supuesto alude a la conducta consistente en hacerse pasar por otra persona carente de existencia real. En este trabajo nos centraremos en la suplantación de identidad y el uso de nombre supuesto que tienen como objetivo causar un perjuicio patrimonial al legítimo titular de los datos o a un tercero, prestando particular atención al fraude de tarjetas en el comercio tradicional y electrónico, que es la forma más común de suplantación de identidad y uso de nombre supuesto[4].

---

[2] El término «identidad» se refiere, en la segunda acepción del Diccionario de la Lengua Española, al «conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás». Ese conjunto de rasgos está integrado básicamente por el nombre y apellidos y la filiación. Ahora bien, en la actualidad el significado contemporáneo del término «identidad» ha asumido una connotación relacionada con el uso de las nuevas tecnologías que va a más allá del significado tradicional, llegando a incluir aspectos como el historial crediticio y de consumo de una persona, sus cuentas bancarias, su afiliación a partidos, sindicatos, seguros, servicios, etc. Es este significado más amplio del término «identidad» el que interesa cuando se conceptualiza la suplantación, usurpación o robo de identidad. Cfr. COLLINS, J., *Preventing Identity Theft Into Your Business*, John Wiley, New Jersey, 2005, p. 7.

[3] No se hará distinción nominal, pues, entre lo que en Estados Unidos se conoce como «*identity theft*», que es el acceso ilícito a datos personales, y el «*identity fraud*», nombre con el que se designa la utilización de los datos así conseguidos para obtener una ganancia ilícita, aunque sí se tendrá en cuenta que la primera conducta suele ser un acto preparatorio de la segunda. Cfr. JAVELIN STRATEGY & RESEARCH, *2008 Identity Fraud Survey Report*, disponible en la página web http://www.idsafety.net/803.R_2008%20Identity%20Fraud%20Survey%20Report_Consumer%20Version.pdf, p. 5 [Fecha de consulta: 9/10/09].

[4] FEDERAL TRADE COMMISSION, *Consumer Fraud and Identity Theft Complaint Data January-December 2005*, 2006, p. 3, disponible en la página web www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf [Fecha de consulta: 9/10/09].

La mayor o menor facilidad para hacerse con los datos necesarios para suplantar la identidad de una persona realmente existente depende en buena medida de la estructura que presentan los mecanismos de identificación de la persona en cada país y de sus puntos vulnerables, que no son creados sino aprovechados por los delincuentes.

Así, por ej., el hecho de que en los Estados Unidos se utilice como dato identificativo fundamental el número de la seguridad social (SSN, *Social Security number*), que no nació con dicho propósito, sino para mantener un adecuado registro de las ganancias, careciendo de sistemas de seguridad adecuados, da lugar a que sea relativamente fácil hacerse pasar por otro simplemente contando con ese número[5]. Por ej., acompañado de la fecha de nacimiento propia y de la madre basta para abrir una cuenta bancaria que se puede usar para blanquear cheques[6].

En España el Documento Nacional de Identidad (DNI), emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita, desde hace más de cincuenta años, la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular. A lo largo de su vida, el Documento Nacional de Identidad ha ido evolucionado e incorporando las innovaciones tecnológicas disponibles en cada momento, con el fin de aumentar tanto la seguridad del documento como su ámbito de aplicación. En la actualidad, las medidas adoptadas contra la falsificación van desde la impresión de la palabra «España» con una tinta ópticamente variable, que se ve magenta o verde al variar el ángulo de observación, hasta un hilo de seguridad, embebido en el papel, que cruza en sentido vertical toda la superficie del DNI y es luminiscente a la luz ultravioleta, pasando por fondos de seguridad para la fotografía en color del titular y la grabación del número del DNI en láser, apreciable al tacto. Pese a estas medidas, existen numerosos casos de falsificación del DNI, sea mediante la alteración de uno legítimo, los menos, sea mediante la elaboración de uno con datos falsos, los más.

Los mismos problemas que tiene el DNI tradicional afectan al pasaporte, al Número de Identificación de Extranjero (NIE), a los permisos de residencia y de trabajo, etc. Ninguno de estos documentos de identificación es completamente seguro.

---

[5] Como apunta CAMP, L. J., *Economics*, cit., p. 18, la eficacia de la suplantación de identidad en los EE.UU. se basa en la fragilidad de un sistema de identidad basado en el número de la Seguridad Social. La constatación de este hecho ha llevado a que legislativamente se haya intentado limitar la utilización de este número como mecanismo de identificación, sin mucho éxito. Vid. los detalles en MAY, D. A./HEADLEY, J. E., *Identity Theft*, Peter Lang, New York, 2004, pp. 12-13.

[6] Vid. diversos datos y estadísticas relativos a esta forma de suplantación de identidad en Hayward, C. L. (Ed.), *Identity Theft*, Novinka Books, New York, 2004, pp. 145-150.

A ello se añade que la mayoría de los mecanismos de identificación y autenticación desarrollados en el mundo real, basados fundamentalmente en el contacto personal entre los sujetos que interactúan y el reconocimiento de la apariencia física o de la firma, no son aplicables al mundo virtual[7].

> Por ello, con la llegada de la Sociedad de la Información y la generalización del uso de Internet se consideró necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad con el fin de poder acreditar electrónicamente y de forma indubitada la identidad de la persona, y que pudiera firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita. Para responder a estas nuevas necesidades nació el Documento Nacional de Identidad electrónico (DNIe), regulado por el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, cuya principal novedad es que incorpora un pequeño circuito integrado (chip), capaz de guardar información y de procesarla internamente. Para incorporar este chip, el DNI cambia su soporte tradicional (cartulina plastificada) por una tarjeta de material plástico, dotada de nuevas y mayores medidas de seguridad. En la medida que el DNIe vaya sustituyendo al DNI tradicional y se implanten las nuevas aplicaciones, podremos utilizarlo para realizar compras firmadas a través de Internet, hacer trámites completos con las Administraciones Públicas a cualquier hora y sin tener que desplazarse ni hacer colas, realizar transacciones con entidades bancarias, participar en una conversación por Internet con la certeza de que nuestro interlocutor es quien dice ser, etc. Por añadidura, según los implicados en su desarrollo este novedoso sistema de identificación resulta virtualmente imposible de falsificar, tan diversos son los elementos que lo constituyen. Medidas de seguridad física perceptibles a simple vista como las tintas ópticamente variables, relieves y fondos de seguridad, o visibles mediante medios ópticos y electrónicos como tintas visibles con luz ultravioleta o microescrituras; así como medidas de seguridad digitales como encriptación de los datos del chip o acceso al mismo mediante PIN, asegurarían un alto nivel de protección hasta hacerlo prácticamente inviolable o falsificable. Ahora bien, los expertos advierten que el DNIe presenta ya problemas de seguridad de los algoritmos y del entorno, en particular cuando se tiene en cuenta que la mayoría de los titulares carece de conocimientos extensos de informática y apenas adoptan medidas de protección del «*hardware*» que emplean en el hogar o en el trabajo, lo que los hace vulnerables a los ataques informáticos orientados a apoderarse de las claves, por ej., a través de un troyano o de un «*keylogger*»[8].

---

[7] Lo pone de relieve gráficamente CAMP, L. J., *Economics*, cit., pp. 5-16.

[8] Cfr. RAMIÓ AGUIRRE, J., «Elementos de inseguridad en el documento nacional de identidad electrónico DNIe», disponible en la página web http://www.criptored.upm.es/guiateoria/gt_m001o.htm [Fecha de consulta: 9/10/09].

Por lo que se refiere a la seguridad de las tarjetas bancarias y comerciales, sólo en tiempos relativamente recientes la industria ha empezado a investigar el tema, debido a su auge como medio de pago tanto en el comercio tradicional como en el electrónico.

En el comercio tradicional se exige, además de la presentación del soporte físico de la tarjeta, que se pasa por el terminal correspondiente, la marcación del PIN en los casos en que resulta necesario, que son cada vez menos, y la firma en el recibo, que el titular se identifique mediante el DNI, el pasaporte o el permiso de conducir. Un comerciante cuidadoso comprueba la identidad mediante la foto y la firma, que debe coincidir con la que aparece en el reverso de la tarjeta en el espacio previsto para ello. Raras veces se para a comprobar otros datos. En ocasiones el comerciante, aun pidiendo un documento de identidad, no se molesta más que en echar un vistazo superficial, sin comprobar tampoco la semejanza de las firmas, lo que facilita el fraude.

En el comercio electrónico se exige habitualmente que el titular proporcione el número de la tarjeta y la fecha de caducidad, pero estos datos no son difíciles de obtener (en ocasiones aparecen, por ej., en los recibos de las transacciones, que se suelen desechar sin tomar medidas de seguridad), por lo que a veces se solicitan otros datos adicionales, como puede ser la fecha de nacimiento del titular o los dígitos de control, que se encuentran en el reverso. Cuando la comunicación entre el comprador y el vendedor tiene lugar por medio del correo electrónico, se asienta sobre el protocolo SMTP («*Simple Mail Transfer Protocol*»), que no es seguro, pues resulta relativamente fácil suplantar la identidad de cualquiera de las partes o acceder al contenido del correo. Cuando se utiliza una página web a través de la cual introducir los datos y realizar el pago, sigue siendo fácil suplantar la identidad del vendedor: basta crear una página web con la misma apariencia e invitar al comprador a conectarse a ella e introducir sus datos; si el comprador no comprueba la URL (dirección) de la página web, sus datos habrán pasado a manos del delincuente. Para facilitar la autenticación y confidencialidad del servidor se utiliza el protocolo SSL («*Secure Socket Layer*»)[9], el cual, no obstante, no garantiza la autenticación del cliente, lo que, por un lado, facilita el fraude en los sitios web que permiten la descarga del contenido y, por otro, no

[9] Vid. una detallada descripción de su funcionamiento en FRAMIÑÁN SANTAS, J., «Medios de pago *on line* a través de Internet», en GÓMEZ SEGADE, J. A. (Dir.), *Comercio electrónico en Internet*, Marcial Pons, Madrid-Barcelona, 2001, pp. 385-386; MARTÍNEZ GONZÁLEZ, M., «Mecanismos de seguridad en el pago electrónico», en MATA Y MARTÍN, R. M. (Dir.), *Los medios electrónicos de pago. Problemas jurídicos*, Comares, Granada, 2007, pp. 52-56. El sistema se basa en un algoritmo que codifica los datos con un cifrado de hasta 128 *bits*, lo que garantiza que aunque se intercepte la comunicación su significado no podrá ser interpretado.

impide que un comerciante deshonesto utilice fraudulentamente los datos de la tarjeta que ha obtenido al realizar una transacción, al igual que tampoco protege al comerciante del riesgo de que la tarjeta esté siendo utilizada por quien no es su titular[10]. Precisamente para evitar el riesgo que supone la entrega de datos al vendedor se está aplicando el protocolo 3-D Secure, desarrollado por VISA. Otra forma de evitar la entrega de datos al vendedor consiste en la utilización del teléfono móvil para autenticar al titular de la tarjeta, a través de proveedores o intermediarios como Mobipay[11]. Más seguro parece el empleo del protocolo SET («*Secure Electronic Transaction*»), que implica la intervención en cada operación de una entidad que actúa como pasarela de pago entre el titular de la tarjeta y el comerciante, una vez que ambas partes se han adherido al sistema. Al adherirse, el comerciante renuncia a recibir los datos relativos a las tarjetas de los clientes que utilizan esta función de pago seguro, que sólo conoce la pasarela de pago, que ignora, no obstante, cuáles son los bienes o servicios adquiridos por el comprador. Por su parte, el comprador no entrega sus datos al comerciante, debiendo utilizar una contraseña específica con el fin de autenticarse y que la pasarela de pagos autorice la operación[12]. Este sistema garantiza la confidencialidad de los datos, la autenticación de todas las partes, que deben estar identificadas mediante certificados digitales, la integridad y el no repudio, mediante el uso de firma digital[13].

Los datos que permiten la suplantación de identidad en el comercio electrónico pueden conseguirse fraudulentamente tanto utilizando medios o procedimientos informáticos, por ej., por medio del empleo de un programa espía («*spyware*»), como otras modalidades menos sofisticadas, por ej., la búsqueda de documentación bancaria o comercial en la basura de otro (lo que se conoce como «*dumpster*

[10] Vid. estos y otros problemas de seguridad del sistema en CAMP, L. J., *Economics*, cit., pp. 52-55.

[11] La forma de funcionamiento es la siguiente: en el momento del pago aparece en la página web la opción de pago con Mobipay. Una vez activada, aparece una referencia en pantalla que el comprador debe introducir en su teléfono móvil, pulsando a continuación la tecla de llamada. El comprador recibe un mensaje en su móvil, en el que constan el nombre del comercio y el importe de la operación, de manera que si está de acuerdo selecciona la tarjeta con la que desea efectuar el pago y confirma la operación, para lo cual necesita marcar su número de identificación personal (un PIN de cinco dígitos). El comercio recibe la confirmación del pago y el comprador un mensaje en su móvil que confirma la operación.

[12] Vid. una detallada descripción de su funcionamiento en FRAMIÑÁN SANTAS, J., «Medios de pago», cit., pp. 374-385. Este sistema de uso de la tarjeta con la certificación de un tercero parece destinado a convertirse en el estándar para el pago seguro en el comercio electrónico. Cfr. CASTILLA CUBILLAS, M., *La tarjeta de crédito*, Marcial Pons, Madrid-Barcelona, 2007, p. 77.

[13] Cfr. ALONSO CONDE, A. B., *Comercio electrónico: antecedentes, fundamentos y estado actual*, Universidad Rey Juan Carlos/Dykinson, Madrid, 2004, pp. 44-46.

diving»[14]) o en su correo postal («*boxing*»[15]), el mero espionaje puramente físico para obtener las claves de acceso al sistema o los datos de identidad («*shoulder surfing*»)[16], una brecha en la seguridad de una entidad o empresa que disponga de los datos[17] o la connivencia con un comerciante deshonesto. Los casos de usurpación de identidad relacionados con el uso de Internet se basan en buena medida en la previa obtención de los datos por medio de ataques a veces muy sofisticados, como el «*phishing*»[18], el «*smishing*»[19], el «*web spoofing*»[20] o el «*pharming*»[21], y a veces más primitivos[22], pero en cualquier caso ma-

---

[14] Vid. la descripción de su funcionamiento en FERNÁNDEZ TERUELO, J. G., «Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de la red», *RDPC* núm.19, enero 2007, pp. 218-219. Estos programas pueden usarse para reunir información confidencial contenida en un ordenador sin que el usuario lo perciba. No son difíciles de encontrar, puesto que se utilizan también con fines lícitos: por ej., para que el empresario pueda controlar el ordenador del trabajador o los padres el del hijo.

[15] Sobre su relación con la suplantación de identidad, vid. FEDERAL DEPOSIT INSURANCE CORPORATION, *Putting an End to Account-Hijacking Identity Theft*, 2004, p. 10, disponible en la página web http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf, [Fecha de consulta: 9/10/09].

[16] Es la sustracción de las tarjetas de crédito enviadas a los titulares por los bancos interceptándolas en los buzones.

[17] Por ej., hay usuarios que tienen en un lugar visible de su lugar de trabajo o en su casa un post-it con su «*login*» y su «*password*», lo que permite a cualquier persona memorizarlos y acceder al sistema suplantando su identidad. Otra modalidad consiste en mirar por encima del hombro mientras se teclea el número secreto de la tarjeta para realizar un pago o extraer dinero del cajero automático o bien, de forma algo más sofisticada, averiguar cuáles son las teclas marcadas esparciendo sobre el teclado una fina capa de material que sólo se ve a la luz ultravioleta.

[18] En la mayoría de los casos debida a ataques internos, procedentes de trabajadores de la entidad o empresa. Cfr. CHAWKI, M./ABDEL WAHAB, M. S., «Identity Theft in Cyberspace: Issues and Solutions», *Lex Electronica* Vol. 11, Nr. 1, 2006, disponible en la página web www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf [Fecha de consulta: 9/10/09], p. 10.

[19] Esto es, la obtención de los datos del usuario normalmente por medio de un correo electrónico engañoso, aparentemente procedente de una persona o entidad de confianza, por ej., su entidad bancaria, en el que se le pide que, por razones de seguridad, confirme los datos de su cuenta o de sus tarjetas.

[20] Es el «*phishing*» por SMS, enviando los mensajes al teléfono móvil.

[21] Consistente en la suplantación de la página web de un organismo público o de una conocida entidad financiera, a la que se redirige al usuario desde el correo engañoso mediante un enlace, con el fin de apoderarse de sus datos de identidad o de los que dan acceso a su cuenta o permiten el uso de sus tarjetas.

[22] Se trata de una técnica más eficaz que las anteriores al prescindir de la ingeniería social (esto es, de la necesidad de manipular a las personas para conseguir que realicen voluntariamente actos que normalmente no realizarían, como la comunicación de sus datos personales o bancarios), consistente en la explotación de una vulnerabilidad en el «*software*» de los servidores DNS o en el equipo del usuario, o en la introducción de un código malicioso (virus o troyano) que permite al delincuente re-

sivos[23], que son prueba, por una parte, de la enorme capacidad del ciberespacio para llegar a una multitud de víctimas potenciales sin necesidad de una interacción personal[24] y, por otra, de las dificultades que encuentran las Fuerzas y Cuerpos de Seguridad para investigar y poner coto a tales actuaciones, relacionadas con las especiales características del medio en que se producen.

No hay que olvidar tampoco la extensión en Internet de servicios que permiten crear identidades digitales, como las redes sociales[25] de carácter personal, dando lugar a que muchos usuarios transfieran parte de su vida social a la red. Piénsese en Facebook, Second Life o MySpace, o en España Tuenti. También se están extendiendo las redes sociales de carácter profesional, como Linkedin o Xing, y en España

---

dirigir un nombre de dominio a una máquina distinta, ofreciendo una página web falsa, pero muy parecida o igual a la original para obtener los datos, generalmente bancarios, de la víctima. Cada página web tiene asignada una dirección IP, formada por cuatro números de valor comprendido entre 0 y 255. Recordar estos números es complicado, por lo que se asigna paralelamente una dirección nemotécnica URI («*Uniform Resource Identifier*»), única para cada web. La conversión de URI a IP es realizada por servidores especializados llamados de DNS («*Domain Name Service*»), usando unas gigantescas tablas con todas las direcciones. Con el fin de ahorrar engorrosas consultas al DNS, el ordenador del usuario guarda una pequeña tabla con las direcciones utilizadas frecuentemente. Si se intercepta y se cambia la información de esta tabla (fichero «*hosts*»), se puede dirigir al usuario hacia la web que quiera el delincuente. También se puede conseguir lo mismo mediante un ataque a los servidores DNS que cambie la tabla de correspondencia, de forma que cualquiera que introduzca una URL de un banco es dirigido hacia una web pirata, pero eso es más complicado.

[23] Piénsese que en muchos casos el español utilizado en el correo electrónico engañoso presenta evidentes faltas de ortografía y errores gramaticales y sintácticos, e incluso a veces no se oculta la dirección del envío, que puede provenir de fuera del país. A ello hay que añadir que tanto las entidades financieras como las asociaciones de consumidores y usuarios advierten en sus páginas web del peligro que suponen estas conductas, y de que no se debe contestar jamás a tales correos. En estos supuestos cabe plantearse si debe protegerse mediante el Derecho penal al usuario que cree que CajaMadrid le envía un correo electrónico desde Bulgaria, en mal español. En otros países la respuesta a esta pregunta es negativa, al entenderse que el engaño no es idóneo y, a mayores, la víctima ha incumplido sus deberes de autoprotección. Así, por ej., en Alemania, como apunta STUCKENBERG, C.-F., «Zur Strafbarkeit von "hising"», *ZStW* 2006, Vol. 118, Heft 4, p. 895.

[24] Por dar un dato, en enero de 2007 el 1,07% de los correos electrónicos pretendía la obtención de información personal del usuario con fines fraudulentos, lo cual da en conjunto una cifra enorme. Cfr. THORHALLSSON, J., «An User Perspective on Spam and Phishing», en MÖLLER, C./AMOUROUX, A. (Ed.), *Governing the Internet Freedom and Regulation in the OSCE Region*, disponible en la página web http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf [Fecha de consulta: 9/10/09], 2007, p. 211. En la base de estos ataques masivos se encuentra la automatización del proceso de envío de correo electrónico. Para más detalles, vid. BERG, T., «The Changing Face of Cybercrime – New Internet Threats create Challenges to Law Enforcement Agencies», *Michigan Bar Journal* June 2007, p. 21, disponible en la página web http://www.michbar.org/journal/pdf/pdf4article1163.pdf [Fecha de consulta: 9/10/09].

> Neurona y eConozco. A menudo este proceso va acompañado de la revelación de datos personales que pueden ser recolectados con propósitos delictivos. A ello se añade el hecho de que la mayoría de los usuarios de Internet utiliza únicamente una serie limitada de servicios muy demandados y que la existencia de motores de búsqueda especializados en la detección de información privada relativa a una persona permite, además de otros usos lícitos, la obtención de datos personales para su posterior empleo con fines fraudulentos.

Un aspecto de la recogida de datos con fines delictivos que conviene tener en cuenta es que la información sobre personas concretas accesible al público normalmente no puede ser utilizada con dichos fines por sí misma, sino únicamente en combinación con otros datos. Por ello, el delincuente está muy interesado en relacionar distintas informaciones relativas a la identidad de la persona objetivo. En esta tarea se ve apoyado, indirectamente, por la tendencia actual en el comercio electrónico, que se aprecia a nivel global, de relacionar identidades digitales con el objetivo de analizar el comportamiento del consumidor y tratar de predecir su conducta futura sobre la base de los datos obtenidos a partir de distintas fuentes mediante técnicas predictivas y proactivas basadas en la inteligencia artificial y en el análisis estadístico, conocidas como minería de datos o «*data mining*»[26]. Como se reconoce en todos los estudios relacionados con esta técnica, la minería de datos puede ser utilizada por el delincuente para seleccionar la víctima más fácil o vulnerable, así como para hacerse con una combinación de datos que normalmente no está a disposición de cualquiera[27], aunque los datos por separado sí

---

[25] Lo ponen de relieve, entre otros, CHAWKI, M./ABDEL WAHAB, M. S., «Identity Theft», cit., p. 3.

[26] Las redes sociales se definen como comunidades de usuarios que establecen relaciones personales o profesionales y que comparten conocimiento y experiencias. Normalmente se apoyan en sitios web abiertos y en construcción permanente que involucran a conjuntos de personas que tienen necesidades e inquietudes comunes y que se unen para intercambiar y fomentar sus recursos. Sobre esta definición y el grado de penetración de estas redes, vid. el *Libro Blanco de los Contenidos Digitales en España 2008*, realizado por la entidad pública empresarial Red.es, adscrita al Ministerio de Industria, Turismo y Comercio, disponible en la página web http://www.red.es/media/registrados/2008-12/1228995952716.pdf?aceptacion=03471bec49c1709b2614ee1fa7051349 [Fecha de consulta: 9/10/09], pp. 130 ss, que define como un reto del sector la protección de la intimidad, privacidad y datos personales de sus usuarios (p. 133). Sobre los problemas que plantean en relación con el tratamiento de datos personales y la suplantación de identidad, vid. CAMP, L. J., *Economics*, cit., pp. 129-136.

[27] Sobre las amenazas que este proceso puede suponer para la sociedad y el individuo, vid. HANSEN, M./MEISSNER, S. (Hrsg.), *Verkettung digitaler Identitäten*, disponible en la página web https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf, [Fecha de consulta: 9/10/09].

aparezcan en diversas bases de datos de acceso libre. Ello supone que el delincuente puede cometer delitos usando la identidad de una persona sin haber utilizado medios ilegales de obtención de los datos relativos a esa identidad[28].

El objetivo que persigue el delincuente con los datos que obtiene puede ser de diversa índole: desde su utilización en el tráfico jurídico-económico para obtener bienes y/o servicios cargando su coste al verdadero titular de los datos («*financial identity theft*») o a su seguro (por ej., médico, obteniendo servicios a los que no se tiene derecho, lo que se conoce como «*medical identity theft*»), hasta el empleo de los datos relativos a la cuenta de correo electrónico para enviar desde ella correos de contenido ilícito, pasando por la petición de nuevas tarjetas cuyo crédito se agota sin que el titular de los datos tenga conocimiento de ellas, el vaciamiento de la cuenta bancaria de la víctima o del crédito de su tarjeta («*business/comercial identity theft*»). La primera modalidad es muy frecuente, en particular en relación con el uso de tarjetas en el comercio tradicional y electrónico o para la obtención de prestaciones de otra naturaleza (por ej., médicas o de seguridad social), y a ella dedicaremos buena parte de esta investigación. Además, el propósito perseguido por el delincuente puede reducirse a la ocultación de su propia identidad, normalmente para huir de la justicia («*criminal identity theft*»[29]), o ampliarse a la usurpación de la identidad de otro en todos los aspectos de la vida diaria («*identity cloning*»).

En este trabajo no se aborda la calificación penal que merece, en su caso, la forma de hacerse con los datos de identidad, normalmente constitutiva de un delito contra la intimidad, a veces en concurso con otras figuras delictivas (delitos relativos a la propiedad industrial, falsedades, etc.), sino únicamente la que cabe dar a los actos que se llevan a cabo con los datos obtenidos o inventados. Como veremos, la situación en España es complicada debido a la ausencia de una figura delictiva específica, lo que ha llevado a que se ofrezcan soluciones muy variadas en la doctrina y la jurisprudencia. En primer lugar se procederá a analizar el delito de usurpación de estado civil, cuya

[28] Cfr., entre otros, HANSEN, M./MEISSNER, S. (Hrsg.), *Verkettung digitaler Identitäten*, cit., p. 4.

[29] GERCKE, M., *Internet-related Identity Theft*, informe para el Consejo de Europa, 2007, p. 7, disponible en la página web http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Internet_related_identity_theft_%20Marco_Gercke.pdf [Fecha de consulta: 9/10/09]. Pone de relieve que si bien los datos necesarios para comprobar la identidad de una persona eran difíciles de localizar cuando el sistema se basaba en el uso del papel, ello ha dejado de ser así desde que existe Internet y programas de búsqueda y tratamiento de datos como aquellos a los que se alude en el texto CAMP, L. J., *Economics*, cit., pp. 8-9.

aplicación resulta dificultosa cuando el delincuente se limita a utilizar la identidad de otra persona en una única operación fraudulenta, sin pretender asumir en todo momento y a todos los efectos la identidad usurpada. Posteriormente se estudiarán los delitos de estafa, distinguiendo entre las conductas que dan lugar a la aplicación de la estafa común y aquellas que entran en el ámbito de aplicación de la estafa electrónica. Finalizaremos con una referencia a los delitos de falsedad, pues la falsificación y/o utilización de documentos de identidad falsos o de los legítimos sustraídos al titular para reforzar la suplantación de identidad dan lugar a una peculiar problemática en este sector de la delincuencia, sin olvidar que la falsificación de tarjetas recibe el mismo tratamiento penal que la de moneda.

II. Posibilidades y límites del delito de usurpación de estado civil

El delito de usurpación de estado civil, recogido en el art. 401, constituye una falsedad personal. Como tal, protege un bien jurídico colectivo constituido por la fe pública, que se puede concretar en la confianza de la comunidad en la correcta identificación de las personas, a su vez instrumento esencial de la vida social y del tráfico jurídico-económico[30].

> De esta forma descarto que se proteja aquí la familia, como afirmaban algunos autores[31], o el estado civil en sí mismo considerado, como apuntaban otros[32].

---

[30] Que permite detectar fallos sistemáticos en la organización de los datos empleados para identificar a los (presuntos) delincuentes. Por ej., si el sistema se centra en la información que sirve para la identificación del delincuente (nombre, apellidos, fecha de nacimiento, número de DNI), que pueden pertenecer a un tercero, y no en los datos biométricos que están a disposición de las fuerzas y cuerpos de seguridad, por ej., las huellas dactilares, esto es, en atributos permanentes que permiten autenticar la identidad, es fácil que se den supuestos de suplantación de identidad para escapar de las consecuencias del delito. Vid. ampliamente CAMP, L. J., *Economics*, cit., pp. 26-32.

[31] Se trata de una opinión mayoritaria. Vid. por todos BOIX REIG, J./JAREÑO LEAL, A., «De la usurpación del estado civil», en VIVES ANTÓN, T. S. (Coord.), *Comentarios al Código Penal de 1995. Volumen II (Art. 234 a Disposiciones Finales)*, Tirant lo Blanch, Valencia, 1997, pp. 1763 ss; GORDILLO ÁLVAREZ-VALDÉZ, I., «Falsedades», en LAMARCA PÉREZ, C. (Coord.), *Derecho Penal. Parte especial*, 4.ª ed. Colex, Madrid, 2008, p. 585; QUINTERO OLIVARES, G., «Artículo 401», en QUINTERO OLIVARES, G. (Dir.), *Comentarios al Código Penal. Tomo III. Parte Especial (Artículos 319 a DF 7.ª)*, 5.ª ed., Thomson-Aranzadi, Cizur Menor, 2008, p. 509.

[32] Por ej., RODRÍGUEZ DEVESA, J. M., *Derecho penal español. Parte especial*, 6.ª ed. Madrid, 1975, pp. 225-226, citando a Groizard.

En este precepto se sanciona la utilización en el tráfico jurídico-económico del nombre y la filiación de otra persona realmente existente, con independencia de que esté viva o haya fallecido[33]. Si la persona cuyo estado civil se usurpa vive, puede constituirse en perjudicado por el delito a efectos de la responsabilidad civil, en su caso[34].

> Un sector doctrinal[35] y jurisprudencial[36] entiende que los fallecidos carecen de estado civil que se pueda usurpar, sin tener en cuenta que no se tutela tanto el estado civil cuanto la fe pública, que se ve afectada por la usurpación con independencia de si la persona vive o no.

Lo que aquí se castiga es, pues, la suplantación de la identidad de otra persona, por lo que podría pensarse que es la figura delictiva perfecta para abarcar buena parte de los supuestos que nos ocupan. Ahora bien, un análisis detenido de la práctica jurisprudencial lleva a concluir que su ámbito de aplicación está restringido a los casos en que se suplanta la identidad de otra persona a todos los efectos, absolviéndose cuando se acredita un uso concreto y determinado con un objetivo también concreto.

El objeto de la acción es el estado civil de otra persona. De acuerdo con el art. 1 de la Ley de 8 de junio de 1957 sobre el Registro Civil, «en el Registro Civil se inscribirán los hechos concernientes al estado civil de las personas y aquellos otros que determina la Ley. Constituyen, por tanto, su objeto: 1. El nacimiento. 2. La filiación. 3. El nombre y apellidos. 4. La emancipación y habilitación de edad. 5. Las modificaciones judiciales de la capacidad de las personas o que éstas han sido declaradas en concurso, quiebra o suspensión de pa-

---

[33] Así, FUENTE HONRUBIA, F. de la, «La usurpación de estado civil», *Actualidad Penal* 2000-1, marg.148, si bien apunta que simultáneamente también se protege la fe pública.

[34] BOIX REIG, J., *El delito de usurpación de estado civil*, Universidad de Valencia, Valencia, 1980, pp. 34-35; BOIX REIG, J./JAREÑO LEAL, A. «De la usurpación», cit., p. 1765; FUENTE HONRUBIA, F. DE LA, «La usurpación», cit., margs.150-151; MORILLAS CUEVA, L., «Falsedades (III). Falsedades personales», en COBO DEL ROSAL, M. (Coord.), *Derecho Penal Español. Parte Especial*, 2.ª ed. Dykinson, Madrid, 2005, p. 851; MUÑOZ CONDE, F., *Derecho Penal. Parte Especial*, 16.ª ed. Tirant lo Blanch, Valencia, 2007, p. 307; QUINTERO OLIVARES, G., «Artículo 401», cit., pp. 509-510.

[35] Cfr. QUINTERO OLIVARES, G., «Artículo 401», cit., p. 509.

[36] BAJO FERNÁNDEZ, M./DÍAZ-MAROTO Y VILLAREJO, J., *Manual de Derecho penal. Parte especial, III*, 3.ª ed. Ceura, Madrid, 1995, p. 325; GORDILLO ÁLVAREZ-VALDÉS, I., «Falsedades», cit., p. 587, y QUERALT JIMÉNEZ, J. J., *Derecho Penal Español. Parte especial*, 5.ª ed. Atelier, Barcelona, 2008, pp. 683-684. En la doctrina más antigua, CUELLO CALÓN, E., *Derecho penal. Tomo II (Parte especial)*, 14.ª ed. Bosch, Barcelona, 1975, p. 728, alegando que «un ser que no existe no posee estado civil alguno».

gos. 6. Las declaraciones de ausencia o fallecimiento. 7. La nacionalidad y vecindad. 8. La patria potestad, tutela y demás representaciones que señala la Ley. 9. El matrimonio. 10. La defunción». Por su parte, el art. 53 del mismo texto señala que «las personas son designadas por su nombre y apellidos, paterno y materno, que la Ley ampara frente a todos», lo que se complementa con el art. 109 Cc, de acuerdo con el cual «la filiación determina los apellidos con arreglo a lo dispuesto en la Ley». En la doctrina existen dos posiciones respecto a si este conjunto de datos recibe por igual protección a través del delito de usurpación de estado civil, pues un sector entiende que sí[37], mientras que otro, mayoritario[38], opta por limitar el objeto de la acción al nombre y filiación que tiene otra persona, con base en que se trata de los únicos datos entre los mencionados que son privativos de una persona determinada e inmodificables, sin perjuicio de las modificaciones que permiten las normas de orden público contenidas al respecto en el Código civil y la Ley sobre el Registro Civil. Con independencia del interés que pueda tener esta discusión, en la jurisprudencia sólo se encuentran sentencias referidas al nombre y filiación.

> Si el autor utiliza un nombre o filiación que legalmente no le pertenecen pero podrían llegar a ser suyos, por ej., mientras está pendiente un proceso para determinar la filiación, la conducta es atípica, pues no usurpa el estado civil «de otro», ya que no «pertenece a nadie pues sólo podría llegar a pertenecerle a él mismo»[39].

En lo que respecta a la conducta típica, el verbo «usurpar» significa, según el Diccionario de la Real Academia, «1. tr. Apoderarse de una propiedad o de un derecho que legítimamente pertenece a otro, por lo general con violencia. 2. tr. Arrogarse la dignidad, empleo u oficio de otro, y usarlos como si fueran propios». En el contexto del art. 401 CP es equivalente a usar como propios el nombre y la filiación de otra persona. Ahora bien, se plantea la duda acerca de si es exigible que con dicho uso se pretenda privar al legítimo titular de algún derecho que le corresponda o causarle algún perjuicio, opción esta que es mayoritaria en la doctrina[40]. En la jurisprudencia se exige que la usurpación suponga la total suplantación de la identidad de otra persona, absolviendo cuando únicamente se acredita un uso

---

[37] STS de 23-5-1986 ssAP de Madrid de 17-3-1999 (ARP 1999\2036) y de Palencia de 12-11-2007 (JUR 2008\94074).

[38] Gordillo Álvarez-Valdés, I., «Falsedades», cit., p. 586.

[39] Así, entre otros, Córdoba Roda, J., «Artículo 401», cit., p. 1878; Morillas Cueva, L., «Falsedades (III)», cit., p. 851; Quintero Olivares, G., «Artículo 401», cit., p. 510.

[40] Quintero Olivares, G., «Artículo 401», cit., p. 512.

concreto y determinado para una finalidad también concreta[41], pues se ha convertido casi en una constante la concepción de la usurpación de estado civil como una subrogación o suplantación de otra persona para usar sus derechos y acciones, de modo que la ausencia de este uso supone la absolución[42]. Otro sector jurisprudencial, no obstante, a mi juicio con mejor criterio, condena en casos en que se suplanta la identidad sin utilizar derechos o acciones de la persona suplantada, ocultándose simplemente la identidad propia con efectos procesales[43].

De acuerdo con el tenor literal del precepto no es necesario que se cause un perjuicio, patrimonial o de otra clase. El tipo penal tampoco exige que la conducta tenga lugar «en perjuicio de» la persona suplantada o para perjudicarla. Sin embargo, la jurisprudencia introduce ese requisito por vía interpretativa, siguiendo una tradición histórica[44].

---

[41] Ya PACHECO, J. F., *El Código Penal. Concordado y comentado*, Edisofer, Madrid, 2000 (reedición de la 3.ª de 1867), p. 1136, afirmaba que usurpar el nombre de otro para sacar un pasaporte, eximirse de alguna vejación o facilitar alguna cosa que ofrece dificultades no es usurpación de estado civil, sino «culpas ligeras, que de ningún modo puede tener presentes la ley cuando imponía un castigo tan grave y tan duro... La usurpación de mero nombre, cuando no se trata de privar al que verdaderamente lo lleva de ningún derecho que le corresponda, no puede constituir la usurpación del estado civil a que se refiere la ley en este artículo».

[42] Se trata de una línea prácticamente constante. Así, entre otras, las SSAP de Salamanca de 2-7-2001 (JUR 2001\250521), en un caso en que los acusados se hacen pasar por otras personas para obtener un préstamo hipotecario, de Cádiz de 9-1-2002 (ARP 2002\190), en un caso en que una persona se hace pasar por su hermano en un proceso penal, llegando a ser condenado con la identidad falsa, o de Madrid de 6-11-2006 (ARP 2007/30), en un caso en que se suplanta la identidad de un trabajador para obtener unas prestaciones sanitarias a las que no se tenía derecho. Sin embargo, condenan en sendos casos de suplantación de la identidad de otro en una relación laboral, en que se ejercen los derechos derivados de ella, las SSAP de Alicante de 21-7-2005 (JUR 2006\4572), que afirma que comete el delito quien, sin necesidad de una usurpación total, ejercita actos de una cierta continuidad y trascendencia que no le corresponden, y de Lleida de 13-12-2007 (JUR 2008\72073), que alega la importancia de la relación laboral, puesto que de ella derivan múltiples derechos y obligaciones; también la STS de 26-12-2005 (RJ 2006\1269).

[43] Por ej., las SSTS de 26-3-1991 (RJ 1991\2378), que absuelve a quien suplantó la identidad de su hermano para escapar de la justicia, y de 20-1-1993 (RJ 1993\133), igualmente absolutoria en relación a la usurpación de estado civil por entender que hacerse pasar por otro en un negocio de compraventa no supone ejercer derechos y acciones de la persona suplantada; también la SAP de Cádiz de 9-1-2002 (ARP 2002\190), que absuelve a quien se hizo pasar por su hermano en un proceso penal, al entender que no utilizó los derechos y acciones de la persona suplantada.

[44] Así, condenan en casos en que el autor se hace pasar por otra persona en un proceso las SSAP de Madrid de 5-12-2000 (JUR 2001\93734) y Albacete de 9-5-2002 (JUR 2002\177899).

En cuanto al tipo subjetivo, sólo es admisible el dolo directo. El sector jurisprudencial que exige que la usurpación de identidad tenga lugar para usar los derechos y acciones del suplantado alude a un elemento subjetivo del injusto, que no aparece expresamente en el tipo penal, consistente en «el propósito de ejercitar derechos y acciones de la persona suplantada»[45]. En la doctrina, un sector doctrinal se manifiesta a favor de la existencia de este elemento subjetivo del injusto[46], mientras que otro lo hace en contra[47]. Este supuesto elemento subjetivo tiene su origen en la necesidad de deslindar los delitos de usurpación de estado civil y de uso público de nombre supuesto en el Código penal de 1944/73. Además de que este problema ya no existe, pues la segunda conducta ha sido destipificada, supone enmendar la plana al legislador introduciendo requisitos que el tipo no exige. Cuestión distinta es que se entienda que la acción típica, «usurpar», supone necesariamente el uso de la identidad usurpada, lo que sólo puede realizarse haciéndose pasar por otro con efectos en el tráfico jurídico-económico[48], pero esta exigencia forma parte del tipo objetivo y no constituye un elemento subjetivo del injusto.

En conclusión, aunque el delito de usurpación de estado civil podría, en principio, aplicarse a los casos de suplantación de identidad, castigando dicha suplantación sin necesidad de que se causara un perjuicio efectivo que, de producirse, podría tenerse en cuenta a través de un concurso de delitos con la infracción patrimonial cometida, el entendimiento que de este delito hacen los tribunales lo dificulta en grado sumo. A ello se añade, en el caso de uso de tarjetas en el comercio presencial y electrónico, que «el uso de un medio de pago sin la autorización del titular sólo puede tener como finalidad que éste desarrolle su función, consistente en servir para la obtención de bienes y servicios, por lo que únicamente puede representar una protección anticipada del patrimonio[49], de manera que parece lógico que el uso fraudulento se contemple dentro de las infracciones contra el patrimonio.

---

[45] Vid. ya PACHECO, J. F., *El Código Penal*, cit., p. 1136. Así, la SAP de Sevilla de 23-5-2000 (ARP 2000\1861), que absuelve en un supuesto en que el usurpador actúa con conocimiento y en beneficio del suplantado.

[46] A veces se afirma que concurre tal elemento subjetivo cuando se interviene en negocios jurídicos que crean obligaciones para la persona suplantada (SAP de Cádiz de 21-7-2005, ARP 2005\707), pero si sólo se suplanta la identidad de otro para un negocio concreto se absuelve (vid. las referencias en la nota núm.41).

[47] GORDILLO ÁLVAREZ-VALDÉS, I., «Falsedades», cit., p. 587, y LASCURAÍN SÁNCHEZ, J. A., «De las falsedades», en RODRÍGUEZ MOURULLO, G. (Dir.), *Comentarios al Código Penal*, Civitas, Madrid, 1997, p. 1080.

[48] QUERALT JIMÉNEZ, J. J., *Parte Especial*, cit., p. 684.

[49] BOIX REIG, J., *El delito*, cit., pp. 36-37.

III. Posibilidades y límites de los delitos de estafa

1. Determinaciones previas

La comisión de defraudaciones basadas en la suplantación de identidad se ha visto favorecida por la introducción de las nuevas tecnologías en las transacciones comerciales, en particular por la utilización de nuevos medios de pago en el comercio tradicional y por la generalización del comercio electrónico, en el que las tarjetas de crédito son el método de pago preferido[50]. Ha surgido una rica casuística jurisprudencial en el marco de los delitos de estafa, a los que me referiré a continuación, incluyendo en este estudio otras conductas también relacionadas con el uso de las nuevas tecnologías para realizar la defraudación que, frente a lo que se podría pensar, no siempre dan lugar a la aplicación del delito de estafa informática, pues en no pocas ocasiones es aplicable la estafa común o algún otro delito patrimonial, como el hurto.

Con carácter previo conviene advertir que los delitos de estafa permiten castigar, con las limitaciones que veremos a continuación, el perjuicio patrimonial sufrido por la víctima, pero no contemplan de forma específica que la maniobra engañosa o la manipulación utilizada para causar ese perjuicio sea precisamente la suplantación de identidad.

2. Estafa

«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» (art. 248.1 CP). De acuerdo con el art. 249 CP, «los reos de estafa serán castigados con la pena de prisión de seis meses a tres años, si la cuantía de lo defraudado excediere de 400 euros», debiendo tenerse en cuenta para la fijación de la pena «el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circuns-

[50] Cfr. en sentido similar VILLACAMPA ESTIARTE, C., «La falsificación de medios de pago distintos del efectivo en el Proyecto de Ley Orgánica de Reforma del CP de 2007: ¿respetamos las demandas armonizadoras de la Unión Europea?», *Diario La Ley* núm.6994, 22 de julio de 2008, p. 5, citando a QUINTERO OLIVARES, G., «La «clonación» de tarjetas y el uso de documentos ajenos», en AA.VV., *La armonización del Derecho penal español: una evaluación legislativa*, Ministerio de Justicia, Madrid, 2006, p. 141.

tancias sirvan para valorar la gravedad de la infracción». En caso de que la cuantía de lo defraudado no supere los 400 euros, se aplica la falta contra el patrimonio que se recoge en el art. 623.4 CP, que castiga con localización permanente de cuatro a doce días o multa de uno a dos meses, entre otros, a «los que cometan estafa... en cuantía no superior a 400 euros».

Estamos ante una figura delictiva que no hace mención expresa alguna a la suplantación de identidad. No obstante, su estudio es interesante en la medida en que en esta tradicional infracción patrimonial encajan toda una serie de conductas en las que, aprovechando el empleo de medios de pago basados en las nuevas tecnologías, se produce un engaño, basado en la suplantación de identidad, que da lugar a la causación de un error en una persona física, que realiza en consecuencia un acto de disposición en perjuicio propio o de tercero. Este análisis resulta necesario para deslindar adecuadamente su ámbito de aplicación del que corresponde a la estafa informática, ya que, como veremos, existen resoluciones contradictorias en la jurisprudencia y posiciones encontradas en la doctrina.

Los supuestos que serán aquí objeto de análisis son los relativos a la utilización de tarjetas bancarias de crédito o de débito u otras tarjetas comerciales no bancarias empleadas como medio o instrumento de pago tanto en el comercio tradicional como en el electrónico por quien no es su titular legítimo, ya que las discrepancias en torno a la calificación de las conductas defraudadoras relacionadas con ellas son notables. Adelanto ya que muchos comportamientos encajan sin excesivas dificultades en la estructura típica del delito común de estafa.

Así, constituye un delito común de estafa la conducta denominada «*carding*», esto es, la utilización de una tarjeta bancaria de crédito o de débito, o cualquier otra que se pueda emplear como medio de pago, como una tarjeta de comercio o un monedero electrónico, perdida por el titular, sustraída al titular u obtenida de éste mediante engaño o fraude, en el comercio tradicional[51]. La presentación de la tar-

[51] Cfr. CASTILLA CUBILLAS, M., *La tarjeta de crédito*, cit., pp. 73-74. En el comercio electrónico español el comerciante propone preferentemente el pago con tarjeta de crédito en el 80% de los casos. Cfr. *Study on the Security of Payment Products and Systems in the 15 Member States, Internal Market DG, Final Report* (Contract n.º. ETD/2002/B5-3001/C/11), de 2003, que se puede consultar en la página web http://ec.europa.eu/internal_market/payments/docs/fraud/study-security/200309-finalreport_en.pdf [Fecha de consulta: 9/10/09], p. 136, gráfico 51. El *Estudio sobre el Comercio Electrónico B2C 2006*, realizado por la entidad pública empresarial red.es, adscrita al Ministerio de Industria, Turismo y Comercio, y la Asociación Española de Comercio Electrónico (AECE-fecemd), disponible en http://observatorio.red.es/

jeta al pago, haciéndose pasar por su titular legítimo, crea una falsa apariencia de crédito ante el comerciante.

En ocasiones se ha considerado estafa informática[52], sin tener en cuenta que se dan todos los elementos de la estafa común y que, por el contrario, falta la manipulación informática o artificio semejante.

---

estudios/documentos/B2C2006.pdf [Fecha de consulta: 9/10/09],p. 37, por su parte, fija el porcentaje de compradores que declara utilizar las tarjetas de crédito o débito para el pago de las compras en Internet en el 48,3%, mientras que el porcentaje de compradores que declara preferir este medio de pago llega al 60,9% en el *Estudio sobre Comercio Electrónico B2C 2007*, elaborado por la misma entidad, y disponible en la página web http://observatorio.red.es/estudios/consumo/index.html [Fecha de consulta: 9/10/09], p. 30. Ahora bien, en el *Estudio sobre Comercio Electrónico B2C 2008*, de la misma entidad y disponible en la página web http://www.red.es/media/registrados/2008-10/1224573484057.pdf?aceptacion=c8fb6587ee8c411f2f0920818dfbc4d8 [Fecha de consulta: 19/10/09], p. 36, se apunta que «la mayoría (54%) de los compradores prefieren pagar sus compras on-line a través de tarjeta de crédito o débito (básicamente crédito). Esta preferencia se mantiene a lo largo de los últimos ejercicios. No obstante, entre los compradores de 2007 la predilección no es tan manifiesta como en años anteriores, dando mayor espacio a otras formas de pago». Entre los jóvenes y los residentes en ciudades de más de 100.000 habitantes se está imponiendo el PayPal como medio favorito de pago en las compras por Internet. A la pregunta de qué habría que mejorar para aumentar las compras en Internet la mayoría de los encuestados, un 40,7%, responde una mayor seguridad en los pagos, y ello «a pesar de la baja incidencia de problemas relacionados con los procesos de pago». Op. et loc. cit., p. 52.

[52] Vid., entre otros, FERNÁNDEZ ENTRALGO, J., «Falsificación y utilización fraudulenta de tarjetas electrónicas», en MAZA MARTÍN, J. M. (Dir.), *Tarjetas bancarias y Derecho penal*, CDJ VI-2002, CGPJ, Madrid, 2003, p. 58; FERNÁNDEZ GARCÍA, E. M., «Los fraudes con tarjetas de pago y otros supuestos de delincuencia informática patrimonial. Incidencia de la Reforma Penal», en AA.VV., *Estudios jurídicos. Ministerio Fiscal. II-2003. Delincuencia Informática. Drogas de abuso: Aspectos Científicos y Jurídicos. Experiencias aplicativas de la LORPM*, Ministerio de Justicia, Madrid, 2004, p. 152; JAVATO MARTÍN, A. M., «Análisis de la jurisprudencia penal en materia de medios electrónicos de pago», en MATA Y MARTÍN, R. M. (Dir.), *Los medios electrónicos de pago. Problemas jurídicos*, Comares, Granada, 2007, p. 371; FERNÁNDEZ TERUELO, J. G., *Cibercrimen. Los delitos cometidos a través de Internet*, CCC, s/l, 2007, pp. 45-46; MATA Y MARTÍN, R. M., «Medios electrónicos de pago y delitos de estafa», en MATA Y MARTÍN, R. M. (Dir.), *Los medios electrónicos de pago. Problemas jurídicos*, Comares, Granada, 2007, pp. 335-336; del mismo autor, *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*, Thomson-Aranzadi, Cizur Menor, 2007, pp. 45-49; RUIZ RODRÍGUEZ, L. R., «Uso ilícito y falsificación de tarjetas bancarias» [artículo en línea]. *IDP. Revista de Internet, Derecho y Política* núm. 3, 2006 [Fecha de consulta: 9/12/08]. http://www.uoc.edu/idp/3/dt/esp/ruiz.pdf>, p. 10; VIVES ANTÓN/GONZÁLEZ CUSSAC en VIVES ANTÓN, T. S. y otros, *Derecho Penal. Parte Especial*, 2.ª ed. Tirant lo Blanch, Valencia, 2008, p. 420. En la jurisprudencia, entre otras, las SSTS de 25-6-1985 (RJ 1985\3056), 19-6-1986 (RJ 1986\3176) y 15-3-1994 (RJ 1994\2317). Más recientemente, las SSTS de 8-7-2002 (RJ 2002\8939), 12-12-2002 (RJ 2003\309), 21-1-2003 (RJ 2003\1032), 30-10-2003 (RJ 2003\7331).

En alguna ocasión se ha aplicado el principio víctimo-dogmático cuando al comerciante le consta que la tarjeta está siendo usada por quien no es su titular, aunque se alegue tener autorización de éste[53], o cuando el comerciante no ha pedido un documento de identificación con el fin de comprobar que la identidad del titular de la tarjeta y la de quien la presentaba para el pago coincidían, cuando habiéndolo pedido no comprueba si la identidad coincide o si la firma coincide con la de la tarjeta, siendo así que la persona firma con nombre y grafía muy diferentes a las del verdadero titular.

> En el primer caso no existe estafa al no estar presente los elementos del engaño y el error. En el segundo caso no existe estafa por ausencia de engaño idóneo, al existir falta de diligencia del comerciante[54].

La existencia de deberes de autoprotección depende de los usos habituales en el sector de que se trate, esto es, puede existir engaño bastante, aunque no se hayan realizado comprobaciones razonables que podrían haber evitado el error, si la conducta del comerciante responde a los usos habituales del comercio.

En estos casos se afirma la estafa[55].

La mera utilización de una tarjeta perdida por el titular u obtenida por un medio constitutivo de infracción penal para extraer dinero de un cajero automático no es estafa común, al no resultar engañada una persona física[56]. Ni siquiera existe estafa cuando el PIN se ha ob-

---

[53] Así, la SAP de Las Palmas de 19-10-1998 (ARP 1998\4072). La critica, con razón, MATA Y MARTÍN, R. M., *Estafa convencional*, cit., pp. 90-91, que considera más acertada la calificación como estafa común.

[54] Hechos probados en la SAP de Girona de 7-6-2001 (JUR 2001\247132).

[55] Así, recogen casos como los apuntados las SSTS de 3-5-2000 (RJ 2000\4881), 2-11-2001 (RJ 2001\9672), y 3-6-2003 (RJ 2003\4286); las SSAP de Segovia de 23-3-1998 (ARP 1998\2085); de Barcelona de 6-3-2001 (JUR 2001\185005), 12-11-2001 (ARP 2001\814) y 1-12-2004 (ARP 2004\725); y de Girona de 17-6-2002 (JUR 2002\225356) y 5-11-2002 (ARP 2003\71), entre otras. En la doctrina, vid. GALLEGO SOLER, J. I., «Fundamento y límites de los deberes de autoprotección de la víctima en la estafa», *ADPCP* Tomo LVIII, Fasc. II, mayo-agosto 2005, pp. 529 ss, en especial p. 538; PÉREZ PELLICER, A., «La estafa de crédito», en BOIX REIG, J. (Dir.), *Estafas y falsedades (Análisis jurisprudencial)*, iustel, Madrid, 2005, pp. 131-132. En la jurisprudencia civil también se niega que responda el titular de la tarjeta por el uso fraudulento por un tercero cuando existe negligencia del establecimiento comercial, por ej., al aceptar un pago con tarjeta sin realizar la debida comprobación de la identidad del usuario. Cfr. BATUECAS CALETRIO, A., *Pago con Tarjeta de Crédito. Naturaleza y régimen jurídico*, Thomson-Aranzadi, Cizur Menor, 2005, pp. 208-209, con citas jurisprudenciales.

[56] Así, la STS de 23-10-2002 (RJ 2002\9604) o la SAP de Segovia de 9-6-2005 (JUR 2005\229950).

tenido engañando al titular, porque aunque hay engaño y error, el titular de la tarjeta no realiza un desplazamiento patrimonial en perjuicio propio, pues es el propio delincuente el que se dirige al cajero automático y provoca el desplazamiento[57]. En mi opinión debe calificarse como estafa informática, pues se suplanta la identidad del verdadero titular. Y subsidiariamente se trataría de un hurto, ya que no cabe duda de que se toma una cosa mueble ajena sin el consentimiento del dueño, que no es la entidad bancaria, sino el titular de la cuenta sobre la que se hace el cargo[58].

Por su parte, se puede calificar como estafa común la conducta denominada «*skimming*», consistente en el uso como medio de pago en el comercio tradicional de una tarjeta legítima que previamente ha sido manipulada para alterar los datos contenidos en la banda magnética[59], modificar el código numérico, el nombre del titular, etc., que obran en el soporte plástico, o bien en el uso de una tarjeta completamente falsa, con datos de una persona inexistente[60]. En el primero de los casos hay suplantación de identidad, pues aunque se borre el nombre del titular para poner el propio lo cierto es que los datos informáticos que el datáfono transmite a la entidad colaboradora son los del titular legítimo, al que se cargará el gasto realizado. En el segundo caso, que se conoce en la práctica norteamericana como «*synthetic identity fraud*», no hay suplantación de identidad de una persona con existencia real, sino creación de una identidad falsa a todos los efectos, si bien a veces se utilizan algunos datos de personas reales.

---

[57] Vid. por ej., ROMEO CASABONA, C. M., *Poder informático y seguridad jurídica*, Fundesco, Madrid, 1988, p. 126; del mismo autor, «Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos», *Poder Judicial* número especial IX, 1988, pp. 114 ss. Antes del Código penal de 1995 sostenía que quien resulta engañada es la entidad bancaria, admitiendo la estafa, MATA BARRANCO, N. de la, «Utilización abusiva de cajeros automáticos: apropiación de dinero mediante la tarjeta sustraída a su titular», *Poder Judicial* núm. especial IX, 1988, pp. 172 ss. Con el Código penal de 1995 admite la estafa en estos supuestos, con la misma argumentación, MATELLANES RODRÍGUEZ, N., «Algunas notas sobre las formas de delincuencia informática en el Derecho penal», en DIEGO DÍAZ-SANTOS, R./SÁNCHEZ LÓPEZ, V. (coords.), *Hacia un Derecho penal sin fronteras*, Colex, Madrid, 2000, p. 141.

[58] Cfr. ROMEO CASABONA, C. M., «Delitos», cit., p. 114.

[59] Y ello con independencia de quién sea la persona efectivamente perjudicada en último término, en virtud de lo que se disponga en el contrato firmado entre el titular de la tarjeta y la entidad emisora, así como de lo que se derive de los contratos de seguro que puedan existir suscritos por el titular o por la entidad emisora en relación a la cobertura del riesgo de uso fraudulento de la tarjeta. Afirma que se trata en todo caso de un hurto CALLE RODRÍGUEZ, M. V., «El delito de estafa informática», *La Ley Penal* núm.37, abril 2007, pp. 54-55.

Existe un sector jurisprudencial que considera que estos supuestos son constitutivos de delito de estafa informática[61], posición que no me parece correcta[62]. En efecto, en este caso la intervención de un sistema informático, como es el asociado al uso de tarjetas para el pago a través de terminales de punto de venta, no es el aspecto decisivo de la conducta, que está constituido por el engaño originado por la apariencia de titularidad legítima y de crédito suficiente que supone la presentación de la tarjeta como medio de pago. El destinatario del engaño y quien sufre el error es una persona física.

Si además de presentar como medio de pago en el comercio tradicional una tarjeta auténtica obtenida ilícitamente o manipulada se imita la firma del titular en la nota de cargo, se aplica habitualmente un delito de falsedad en documento mercantil en concurso medial con un delito o falta de estafa[63].

---

[60] La introducción de las tarjetas dotadas con chip, en lugar de banda magnética, ha permitido que se vaya reduciendo esta forma de fraude. Cfr. CASTILLA CUBILLAS, M., *La tarjeta de crédito*, cit., pp. 70-71.

[61] Vid. por ej., la SAP de Santa Cruz de Tenerife de 3-2-2003 (JUR 2003\140949), que apunta que «la creencia, determinada por el engaño que para los vendedores suponían la presentación de las tarjetas de crédito visa, como auténticas y que respondían a un depósito dinerario real, y la falsa identidad del acusado que acudía como comprador, fue lo que determinó a los vendedores a la entrega…, que supone el desplazamiento patrimonial, que provoca, enriquecimiento en una parte y perjuicio en la otra, lo que configura el delito de estafa» (FJ 1°). En el mismo sentido, la SAP de Madrid de 18-7-2005 (JUR 2005\258245), la SAN de 17-7-2006 (ARP 2006\713) y la STS de 8-7-2002 (RJ 2002\8939).

[62] Así, la SAP de Las Palmas de 19-10-1998 (ARP 1998\4072), que condena por estafa informática al entender que «se asegura la operación mediante una «firma electrónica» coincidente con la clave identificativa que figura en la banda magnética de las tarjetas» (FJ 3°), lo que apartaría la conducta del ámbito de la estafa común. Vid. también las SSAP de Tarragona de 8-6-1998 (ARP 1998\3062) y Palencia de 27-2-2004 (ARP 2004\172, FJ 2°).

[63] Recogen supuestos de hecho similares, entre otras, la SAP de Málaga de 25-6-2005 (ARP 2005\19), en la que tras fabricarse una auténtica nueva tarjeta de crédito manipulando una procedente de previa sustracción o extravío en cuya banda magnética graban un número distinto al original correspondiente a otra tarjeta distinta, los sujetos la utilizan en el comercio engañando al dependiente y accediendo así al terminal de punto de venta; la SAP de Madrid de 17-11-2004 (JUR 2004\254584), FJ 2°, en la que se usa una tarjeta falsificada en la que la banda magnética se correspondía a una real, pero el titular aparente no; la SAN de 10-3-2001 (JUR 2001\170088), FJ 4°, en la que se copian los datos codificados grabados electrónicamente en la banda magnética de las tarjetas que estaban siendo empleadas por sus titulares en un establecimiento comercial, en tarjetas en blanco a nombre de los defraudadores, que fueron utilizadas para pagar diversas compras que éstos realizaron; la STS de 8-7-2002 (RJ 2002\8939).

En la doctrina pone en duda que sea aplicable a estos supuestos la estafa informática, por entender que «la manipulación de la tarjeta no equivale a la manipulación del sistema informático», aunque más adelante apunta que se «ha intervenido en el

> De acuerdo con el art. 77 CP, en caso de que una infracción sea medio necesario para cometer la otra, se aplica «en su mitad superior la pena prevista para la infracción más grave, sin que pueda exceder de la que represente la suma de la que correspondería aplicar si se penaran separadamente las infracciones». La infracción más grave en el concurso que nos ocupa es la falsedad en documento mercantil cometida por particular, pues además de la pena de prisión de seis meses a tres años, que coincide con la del delito de estafa, prevé adicionalmente una multa de seis a doce meses. La mitad superior de estas penas es prisión de un año, nueve meses y un día a tres años y multa de nueve meses y un día a doce meses.

Téngase en cuenta que, en ocasiones, cuando al comerciante le consta que quien firma no es el titular, la jurisprudencia ha entendido que no existe delito de falsedad en documento mercantil alegando que, puesto que se necesita, «para que la falsedad sea penalmente relevante, además de la concurrencia de los elementos típicos, el concurso del requisito de la antijuridicidad material, consistente en que la falsedad tenga aptitud para lesionar o poner en peligro el bien jurídico protegido por el delito, cual es la fe pública o confianza que la sociedad deposita en el valor probatorio de los documentos... cuando la mendacidad llevada a cabo en el documento no resulte idónea para quebrantar la confianza depositada en su contenido, no produciéndose, en consecuencia, una lesión o puesta en peligro del bien jurídico protegido, dicha mendacidad carece de relevancia penal»[64].

---

sistema quebrantando los mecanismos de protección dispuestos, precisamente, para evitar el acceso por vías no autorizadas», CHOCLÁN MONTALVO, J. A., «Infracciones patrimoniales en los procesos de transferencia de datos», en MORALES GARCÍA, O. (Dir.), *Delincuencia informática. Problemas de responsabilidad*, Cuadernos de Derecho Judicial IX-2002, CGPJ, Madrid, 2002, pp. 270-271; del mismo autor, «Fraude informático y estafa por computación», en LÓPEZ ORTEGA, J. J. (Dir.), *Internet y Derecho penal*, CDJ X-2001, CGPJ, Madrid, 2001, pp. 349-350.

[64] Así, FERNÁNDEZ ENTRALGO, J., «Falsificación», cit., pp. 58-59; JAVATO MARTÍN, A. M., «Análisis», cit., pp. 372-373; FERNÁNDEZ GARCÍA, E. M./LÓPEZ MORENO, J., «La utilización indebida de tarjetas de crédito en el Código Penal de 1995», *Revista del Poder Judicial* núm.46, 1997, p. 196; ORTS BERENGUER, E./ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia, 2001, p. 66; ROMEO CASABONA, C. M., «Delitos», cit., p. 113. También MATA Y MARTÍN, R. M., *El delito de robo con fuerza en las cosas*, Tirant lo Blanch, Valencia, 1995, p. 313, nota 789; del mismo autor, *Delincuencia informática y Derecho penal*, Edisofer, Madrid, 2001, p. 57; del mismo autor, *Estafa convencional*, cit., p. 48.

Vid. en este sentido las SSTS de 25-6-1985 (RJ 1985\3056), 19-6-1986 (RJ 1986\3176) y de 15-3-1994 (RJ 1994\2317). Tras la entrada en vigor del Código penal de 1995, las SSTS de 20-11-2001 (RJ 2002\805), 3-5-2000 (RJ 2000\4881), que absuelve por la estafa, y 27-5-2000 (RJ 2000\5217), ésta analizando la naturaleza jurídica de las notas de cargo que emiten las terminales de punto de venta, para concluir que son documentos mercantiles.

La presentación de un documento de identidad auténtico pero perteneciente a otra persona, para reforzar el engaño, no recibe sanción en nuestro Ordenamiento jurídico, como veremos con más detalle al estudiar los delitos de falsedad. Cuestión distinta es que para reforzar el engaño se exhiba un documento de identidad previamente falsificado por un tercero, pues en este caso el concurso se completa con el delito de uso de documento falso (art. 393, normalmente en relación con el art. 392 CP)[65].

> En este caso, aplicando de nuevo la regla contenida en el art. 77 CP, el delito más grave es la estafa, ya que el uso de documento falso se castiga con la pena inferior en grado a la señalada a los falsificadores, y para la falsificación de documento oficial por particular se prevé una pena de prisión de seis meses a tres años y multa de seis a doce meses, siendo la pena inferior en grado prisión de tres a seis meses menos un día y multa de tres a seis meses menos un día, por tanto menos grave que la correspondiente a la estafa, prisión de seis meses a tres años. La mitad superior de esta pena es prisión de un año, nueve meses y un día a tres años.

Si en lugar de utilizar una tarjeta auténtica ilícitamente obtenida se fabrica una nueva, con datos reales o no, o se altera una existente, son aplicables los delitos de falsificación de moneda, como se verá con detalle más adelante. En caso de que quien falsifica la tarjeta sea la misma persona que posteriormente la utiliza para cometer estafa, existe un concurso medial de delitos entre la falsificación de moneda y la estafa[66].

> En este caso, aplicando el art. 77 CP, el delito más grave es el de falsificación de moneda, que se castiga con prisión de ocho a doce años. Como veremos en su momento, la multa del tanto al décuplo del valor aparente de la moneda, también prevista en el art. 368 CP, no se considera aplicable en la falsificación de tarjetas bancarias, que carecen de valor facial.

Críticamente, por entender que en este concurso medial se valora dos veces la idoneidad del documento falso para inducir a error, una en la falsedad y otra en la estafa, QUINTERO OLIVARES, G., «Fraudes y defraudaciones ante una reforma del Código penal», en ARROYO ZAPATERO, L., y otros, *La reforma del Código penal tras 10 años de vigencia*, Thomson-Aranzadi, Cizur Menor, 2006, pp. 91-93, que propone introducir una regla concursal según la cual se castigaría solamente la estafa cuando el medio utilizado para causar el engaño es una falsedad en documento mercantil o privado.

[65] SAP de Girona de 7-6-2001 (JUR 2001\247132), FJ 2º.

[66] Cfr. FERNÁNDEZ ENTRALGO, J., «Falsificación», cit., p. 59; ROMEO CASABONA, C. M., «Delitos», cit., p. 113.

3. Estafa informática

Entre los delitos contra el patrimonio cometidos por medio de sistemas informáticos destaca la estafa informática, castigada en el art. 248.2 CP, cuyo tenor literal es el siguiente: «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».

La necesidad de regular expresamente este supuesto se afirmaba con carácter general en la doctrina anterior a la entrada en vigor del Código penal de 1995[67], si bien no faltaban opiniones que la matizaban, en el entendimiento de que la actualización de los elementos de la estafa permitiría abarcar los supuestos de estafa informática dentro de la estafa común[68]. En cualquier caso, el Código penal de 1995 puso fin a la polémica con la introducción del art. 248.2 CP, que se configura como una estafa específica en la que, al igual que sucede, por ejemplo, con las figuras contenidas en el art. 251 CP, se equiparan a la estafa a efectos penológicos conductas que carecen de alguno

[67] Así, las SSTS de 10-6-1991 (RJ 1991\4556) y 15-3-1994 (RJ 1994\2317).

[68] La postura clásica en torno al delito de estafa negaba que se pudiera engañar a una máquina. Vid. por todos ANTÓN ONECA, J., *Las estafas y otros engaños*, Seix, Barcelona, 1957, p. 10; PÉREZ MANZANO en BAJO FERNÁNDEZ, M. (Dir.), *Compendio de Derecho Penal (Parte Especial)*, II, Ceura, Madrid, 1998, p. 455. Ahora bien, tampoco faltaron otras objeciones referidas a los demás elementos del delito de estafa, desde la inexistencia de error hasta la necesidad de que los diversos elementos se den en el orden establecido por el tipo. Cfr., entre otros, BACIGALUPO ZAPATER, E., «Utilización abusiva de cajeros automáticos por terceros no autorizados», *Poder Judicial* núm. especial IX, 1988, p. 90, con ulteriores indicaciones bibliográficas; CONDE-PUMPIDO FERREIRO, C., *Estafas*, Tirant lo Blanch, Valencia, 1997, pp. 215-217, que rechaza la estafa por entender que no existe acto de disposición; ROMEO CASABONA, C. M., *Poder informático*, cit., pp. 58-74; VALLE MUÑIZ/QUINTERO OLIVARES en QUINTERO OLIVARES, G. (Dir.), *Comentarios a la Parte Especial del Derecho Penal*, 7.ª ed. Thomson-Aranzadi, Cizur Menor, 2008, pp. 647-648, que afirman que se desfiguraría el engaño, habría que renunciar al error como elemento autónomo y se dilataría en exceso el concepto de disposición patrimonial, con el fin de que abarcara cualquier respuesta automatizada a la manipulación informática. En general se afirmaba la existencia de una laguna punitiva, pues también otras figuras delictivas como el hurto, la apropiación indebida o las falsedades, se mostraban incapaces de abarcar todos los supuestos considerados necesitados de punición. Vid. por todos GONZÁLEZ RUS, J. J., «Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», *Poder Judicial* núm. especial IX, 1988, pp. 48 ss.; HERRERA MORENO, M., «El fraude informático en el derecho penal español», *Actualidad Penal* 2001-3, margs. 940 ss.; ORTS BERENGUER, E./ROIG TORRES, M., *Delitos informáticos*, cit., p. 62; VIVES ANTÓN/GONZÁLEZ CUSSAC en VIVES ANTÓN, T. S., y otros, *Parte Especial*, 2.ª ed. cit., p. 493.

o varios de los elementos propios de la estafa común[69], no siendo posible, por lo tanto, acudir al concepto que recoge el art. 248.1 CP para interpretarlas, pero que suponen en general una actuación subrepticia, astuta, que el legislador ha considerado equiparable al engaño característico de la estafa.

> Así pues, estamos ante una figura autónoma respecto de la estafa, a la que sólo se equipara a efectos penológicos, si bien es cierto que la comparación con la estafa común o genérica sirve, en todo lo que no se diferencia de la informática, como punto de contraste y comparación con la regulación de esta última[70].

Frente a la estafa común, además de por la ausencia de engaño y error, la conducta típica de la estafa informática se caracteriza por el hecho de que la disposición patrimonial se consigue valiéndose el autor «de alguna manipulación informática o artificio semejante»[71]. Por su parte, el acto de disposición patrimonial, en este caso la transferencia de activos patrimoniales, no es realizado por la víctima del engaño, como en la estafa común, pues aquí no suele haber contacto humano, sino por el propio autor a través del sistema[72]. Consecuen-

---

[69] Cfr. GUTIÉRREZ FRANCÉS, M. L., *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991, pp. 341 ss., 409 ss.; de la misma autora, «Delincuencia económica e informática en el nuevo Código Penal», en GALLARDO ORTIZ, M. A. (Dir.), *Ámbito jurídico de las tecnologías de la información*, CGPJ, Madrid, CDJ XI-1996, pp. 264-270; y MATA BARRANCO, N. DE LA, «Utilización abusiva», cit., pp. 172 ss, quienes proponían entender que la estafa no supone necesariamente una relación directa y personal entre dos seres humanos, pudiendo afirmarse que las máquinas no sufren engaño alguno ni realizan el acto de disposición por error, pero que en efecto quien al final sufre un engaño es una persona, aunque no sea directa ni personalmente.

[70] En este sentido, apunta la STS de 21-12-2004 (RJ 2004\8252) que «el tipo penal del art. 248.2 CP tiene la función de cubrir un ámbito al que no alcanzaba la definición de la estafa introducida en la reforma de 1983. La nueva figura tiene la finalidad de proteger el patrimonio contra acciones que no responden al esquema típico del art. 248.1 CP, pues no se dirigen contra un sujeto que pueda ser inducido a error».

[71] Así, entre otros, HERRERA MORENO, M., «El fraude informático», cit., margs. 950-951; SUÁREZ GONZÁLEZ en RODRÍGUEZ MOURULLO, G. (Dir.), *Comentarios al Código penal*, Civitas, Madrid, 1997, pp. 710-711; VALLE MUÑIZ/QUINTERO OLIVARES en QUINTERO OLIVARES, G. (Dir.), *Comentarios a la Parte Especial*, 7.ª ed. cit., pp. 646-647; VIVES ANTÓN/GONZÁLEZ CUSSAC en VIVES ANTÓN, T. S. (coord.), *Comentarios al Código Penal de 1995. Volumen II (Art. 234 a Disposiciones Finales)*, Tirant lo Blanch, Valencia, 1996, p. 1237. Considera que «resulta posible afirmar una equivalencia de los elementos —sin identificación total— y de la secuencia típica», MATA Y MARTÍN, R. M., *Estafa convencional*, cit., p. 63; del mismo autor, «Medios electrónicos de pago», cit., p. 341.

No obstante, la cuestión relativa a las relaciones entre la estafa común y la informática no es pacífica. Vid. un resumen de la discusión en GALÁN MUÑOZ, A., *El fraude y la estafa mediante sistemas informáticos. Análisis del art. 248.2 CP*, Tirant lo Blanch, Valencia, 2005, pp. 285-333, quien fundamenta su propia posición en las pp. 791-809.

temente, se exige que se trate de una transferencia «no consentida», elemento que no está presente en la estafa común porque allí el acto de disposición es llevado a cabo por el sujeto pasivo del delito en perjuicio propio, con consentimiento viciado por el error, o por el sujeto pasivo de la acción en perjuicio de tercero, siendo irrelevante que el tercero haya consentido o no. El hecho de que nos encontremos, de esta manera, ante una conducta subrepticia[73] que da lugar a una transferencia de activos patrimoniales realizada sin consentimiento del titular[74], aproxima la forma de comisión de esta figura delictiva más al hurto que a la estafa[75].

> Pese a ello, no cabe duda de que existen diferencias. La más importante, que el objeto material del delito de estafa informática puede carecer de corporeidad, mientras que en el hurto se trata de una cosa mueble que necesariamente ha de ser susceptible de apoderamiento físico. Ello afecta al momento de la consumación, que en el hurto tiene lugar cuando se puede disponer de la cosa, mientras que en la estafa informática la disposición material puede llegar a no producirse nunca. Por otra parte, el bien jurídico protegido en la estafa informática, al igual que en la estafa común, es el patrimonio, mientras que en el hurto se trata de la propiedad o la posesión.

En relación a la interpretación de los elementos típicos, destaca el hecho de que la acción típica, perfectamente delimitada en la estafa común, que es un delito de resultado con modalidades determinadas

---

[72] Como afirma la STS de 20-11-2001 (RJ 2002\805), «el engaño, propio de la relación personal, es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante».

[73] Carece de relevancia que el delito lo cometa una persona con autorización o legitimada para acceder al sistema informático o una que acceda ilícitamente. Cfr. ORTS BERENGUER, E./ROIG TORRES, M., *Delitos informáticos*, cit., p. 63; VIVES ANTÓN/GONZÁLEZ CUSSAC en VIVES ANTÓN, T. S., y otros, *Parte Especial*, 2.ª ed. cit., p. 494.

[74] En la cuarta acepción de «manipular» en el Diccionario de la Lengua Española se contiene: «*fig.* intervenir con medios hábiles y a veces arteros en la política, en la sociedad, en el mercado, etc., con frecuencia para servir los intereses propios o ajenos».

[75] El consentimiento del titular desempeña aquí la misma función que en el hurto, esto es, da lugar a la atipicidad de la conducta. Cfr. ANARTE BORRALLO, E., «Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información», *Derecho y conocimiento. Anuario Jurídico sobre la Sociedad de la Información* Vol. 1, 2001, p. 236. No faltan autores para los que esta alusión expresa a la ausencia de consentimiento es superflua. Vid. por todos SUÁREZ GONZÁLEZ en RODRÍGUEZ MOURULLO, G. (Dir.), *Comentarios*, cit., p. 711. Lo cierto es que la falta de consentimiento se deduce del procedimiento ilícito seguido para conseguir la transferencia, sin tener que recurrir a presunciones. En este sentido, cfr. GONZÁLEZ RUS, J. J., «Protección penal de sistemas, elementos, datos, documentos y programas informáticos», *RECPC* 01-14 (1999), http://criminet.ugr.es/recpc/recpc_01-14.html [Fecha de consulta: 19/10/09], III.1; HERRERA MORENO, M., «El fraude informático», cit., marg. 959.

de acción, queda abierta, se puede decir que en exceso, en la estafa informática: no sólo el concepto de «manipulación informática» es susceptible de múltiples interpretaciones[76], sino que la coletilla, «u otro artificio semejante», sin duda introducida para no dejar al margen ningún posible desarrollo tecnológico en el futuro[77], abre el tipo hasta el punto de que se puede afirmar que es un delito de resultado[78] que en cuanto a la acción literalmente sólo exige que se realice algún artificio que, como veremos, debe ser necesariamente de naturaleza informática.

En lo que respecta a qué se entiende por manipulación informática, resulta aplicable, en mi opinión, la descripción que se contiene en el art. 3 de la Decisión marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, de acuerdo con el cual «cada Estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada: realización o provocación de una transferencia de dinero o de valor monetario que cause una pérdida no autorizada de propiedad a otra persona, con el ánimo de procurar un beneficio económico no autorizado a la persona que comete el delito o a terceros, mediante: - la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, o - la interferencia indebida en el funcionamiento de un programa o sistema informáticos». Tomando como base tal instrumento internacional, debe entenderse que constituye manipulación informática la introducción, alteración, borrado o supresión indebidos de datos informáticos, especialmente datos de identidad, y la interferencia indebida en el funcionamiento de un programa o sistema informáticos[79].

---

[76] Cfr., entre otros, GALÁN MUÑOZ, A., *El fraude*, cit., p. 616, nota núm.1031; PASTOR MUÑOZ en SILVA SÁNCHEZ, J. M. (Dir.), *Lecciones de Derecho penal. Parte especial*, 2.ª ed. Atelier, Barcelona, 2009, p. 221; SUÁREZ GONZÁLEZ en RODRÍGUEZ MOURULLO, G. (Dir.), *Comentarios*, cit., p. 710.

[77] Es una expresión que se ha entendido referida «al manejo manual, al control, o a la operación sobre algo desvirtuando su auténtico sentido de forma hábil e interesada: algo que aunque de modo muy difuso conlleva, de todos modos, más que una mera alteración» (ANARTE BORRALLO, E., «Incidencia», cit., p. 232, que más adelante insiste en que se trata de una «actividad modificativa mendaz o subrepticia, una «utilización irregular» de un sistema informático, de sus presupuestos básicos o de las órdenes que recibe de modo que produzca resultados no previstos o que de conocerlos no se habrían autorizado», p. 234).

[78] Cfr. CHOCLÁN MONTALVO, J. A., «Estafa por computación y criminalidad económica vinculada a la informática», *AP* 1997-2, marg.1080; VALLE MUÑIZ/QUINTERO OLIVARES en QUINTERO OLIVARES, G. (Dir.), *Comentarios a la Parte Especial*, 7.ª ed. cit., p. 649.

[79] ANARTE BORRALLO, E., «Incidencia», cit., p. 231, afirma que «habríamos pasado de un delito característico de medios comisivos determinados a uno cuasi-resultativo».

> Siguiendo un entendimiento estricto de manipulación informática, defendido por un sector doctrinal, la conducta consistente en usurpar la identidad de otro en transacciones electrónicas mediante el uso no autorizado de sus datos se consideraría únicamente delito de falsedad en concurso, en su caso, con un delito de usurpación de estado civil[80]. Sin embargo, esta noción más amplia de manipulación informática, que abarca la introducción de datos del titular real, sin su consentimiento, ha recibido el beneplácito de la jurisprudencia, como veremos, y responde a las tendencias internacionales en esta materia.

Por tanto, se incluyen tanto la introducción de datos falsos como la introducción indebida, por no estar autorizada, de datos reales, auténticos, en el sistema, pasando por la manipulación de los ya contenidos en él en cualquiera de las fases de proceso o tratamiento informático, así como las interferencias que afectan al propio sistema o programa[81].

> De acuerdo con esta interpretación, cuando por medios informáticos, por ej. introduciéndose en el sistema informático de una entidad bancaria o empleando un programa espía, o no informáticos, por ej., buscando en la basura de otro, se obtiene la identidad del titular y el número de la tarjeta, incluyendo fecha de caducidad y número de control, su utilización para hacer una compra de comercio electrónico cuyo importe se cargará al titular de la tarjeta (el llamado

[80] Como es sabido, las decisiones marco carecen del efecto directo de las directivas. Ello no obstante, recientemente se ha admitido en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas, a partir de la sentencia de 16 de junio de 2005, asunto Pupino (C-105/03), la obligación de los jueces y tribunales nacionales de interpretar el Derecho nacional conforme a las disposiciones contenidas en las decisiones marco. Sobre los límites al principio de interpretación conforme a las decisiones marco, vid. MANES, V., «La incidencia de las «decisiones marco» en la interpretación en materia penal: perfiles de derecho sustantivo», *RECPC* (en línea) núm.09-07, disponible en la página web http://criminet.ugr.es/recpc/09/recpc09.html [Fecha de consulta: 19/10/09], pp. 1-20; MUÑOZ DE MORALES ROMERO, M., «La aplicación del principio de interpretación conforme a las decisiones-marco: ¿hacia el efecto directo?: especial referencia al caso *Pupino*», en ARROYO ZAPATERO, L./NIETO MARTÍN, A. (Dirs.), *El Derecho penal de la Unión Europea. Situación actual y perspectivas de futuro*, Ediciones de la Universidad de Castilla-La Mancha, Cuenca, 2007, pp. 308 ss. A mi juicio, con la interpretación propuesta en el texto no se vulnera ninguno de esos límites, y en particular no se vulneran los que prohíben la analogía «*in malam partem*» y la extensión «*extra legem*» del tipo penal en perjuicio del acusado, ya que tanto «manipulación informática» como «otro artificio semejante» se prestan a una interpretación amplia sin vulneración de los límites mencionados.

[81] Como hemos visto, en la jurisprudencia se exige que la usurpación suponga la total suplantación de la identidad de otra persona, absolviendo cuando únicamente se acredita un uso concreto y determinado para una finalidad también concreta. Es evidente que este entendimiento impide que se aplique el precepto en los casos en que se usurpa la identidad de otro en una única ocasión.

«*card-not-present fraud*») es, en mi opinión, estafa informática por manipulación informática, ya que hay manipulación, pues aunque el sistema informático funciona correctamente y los datos introducidos son reales, se utilizan sin consentimiento del titular[82]. La calificación de esta conducta, sin embargo, no es pacífica en la doctrina. Para algunos autores se trata de una estafa común[83]. A mi juicio, ni se engaña a una persona física ni la transferencia del activo patrimonial es realizada por la víctima o un tercero a consecuencia del error ocasionado por el engaño, sino por el propio autor, por lo que la conducta no encaja en el delito común de estafa. Para otros se trata de una conducta falsaria impune, ya que los datos se hacen constar «en algún tipo de documento, aunque sea electrónico, y en ese supuesto nos encontramos ante una conducta que sería constitutiva de falsedad, pero de la llamada «ideológica» (cometida por particular en un documento mercantil o de otra clase) y por lo tanto sin una expresa tipificación quedaría fuera del derecho penal»[84]. Sin embargo, los datos no son falsos, sino que se utilizan sin consentimiento del titular, que es cosa distinta.

Tampoco encaja en el delito común de estafa la utilización de datos obtenidos por el delincuente mediante «*phishing*», «*web spoofing*» o «*pharming*» para realizar una transferencia patrimonial a su favor, como afirma algún autor[85], pues, además de que en ocasiones el engaño no es idóneo para causar el error, como hemos visto, o directamente no hay engaño alguno, al producirse simplemente una manipulación informática de la que el usuario no es consciente[86], en esta

[82] Ya incluía todos estos aspectos, antes de la aparición del delito que nos ocupa en el Código penal de 1995, ROMEO CASABONA, C. M., *Poder informático*, cit., pp. 47-51. Se acogen a esta descripción, entre otros, HERRERA MORENO, M., «El fraude informático», margs. 954-956; MAGALDI PATERNOSTRO en CÓRDOBA RODA, J./GARCÍA ARÁN, M. (Dirs.), *Comentarios al Código penal. Parte especial. Tomo I*, Marcial Pons, Madrid-Barcelona, 2004, p. 771; ORTS BERENGUER, E./ROIG TORRES, M., *Delitos informáticos*, cit., p. 64; VELASCO NÚÑEZ, E., «Estafa informática y banda organizada. *Phishing, pharming, smishing* y "muleros"», *La Ley Penal* núm.49, mayo 2008, pp. 20-21. Mantiene una posición distinta QUERALT JIMÉNEZ, J. J., *Parte especial*, 5.ª ed. cit., p. 481, para quien la manipulación supone la alteración de los programas o del «*hardware*», dejando la introducción indebida de datos auténticos o su alteración en el artificio análogo.

[83] En este sentido, las SSTS de 26-6-2006 (RJ 2006\4925) y 9-5-2007 (RJ 2007\3577). Expresamente en contra, FERNÁNDEZ TERUELO, J. G., *Cibercrimen*, cit., pp. 48-49; del mismo autor, «Respuesta penal», cit., pp. 239-242.

[84] Cfr. MATA Y MARTÍN, R. M., *Delincuencia informática*, cit., p. 57. En contra, apuntando que el engaño no es idóneo, habiendo falta de diligencia del comerciante, que no comprueba que quien realiza la operación es el titular de la tarjeta, la SJP de Málaga de 19-12-2005 (ARP 2006\43), que también niega la aplicación de la estafa informática por no haber manipulación, declarando la conducta atípica.

[85] QUINTERO OLIVARES, G., «Fraudes», cit., p. 99.

[86] Cfr., por ej., FERNÁNDEZ TERUELO, J. G., *Cibercrimen*, cit., p. 43; del mismo autor, «Respuesta penal», cit., p. 233.

figura delictiva es el propio engañado quien realiza el acto de disposición patrimonial que le perjudica a él o a un tercero, señalándose habitualmente en la doctrina que «el daño patrimonial requerido por la descripción típica es consecuencia directa de la propia disposición realizada por el sujeto engañado», de modo que «entre esta conducta y el resultado no debe mediar un acto delictivo que pudiese ser calificado como de apoderamiento»[87]. En el «*phishing*», sin embargo, el engañado se limita a proporcionar los datos que dan acceso a su patrimonio, pero no realiza disposición patrimonial alguna, siendo necesario un acto de apoderamiento por parte del delincuente, materializado en el uso de los mencionados datos. Y en el «*pharming*» ni siquiera es la víctima o un tercero quien proporciona los datos, sino el «*software*» malicioso instalado sin su conocimiento, pudiendo ser de aplicación, en su caso, los delitos contra la intimidad. Se plantea una situación distinta cuando es la víctima del engaño quien realiza el acto de disposición patrimonial. Así ocurre, por ej., en los casos en que se le envía un correo electrónico informándole de que ha ganado en una lotería «*on line*», y para proceder al pago del premio es necesario que desembolse una cierta cantidad. Si lo hace a consecuencia del error en el que incurre debido al engaño, se habrá consumado una estafa común.

La dificultad de encaje de alguno de estos comportamientos en la estafa común, y la existencia de una interpretación restrictiva de la estafa informática, que limita la manipulación a los casos en que se produce una interferencia en el funcionamiento del sistema o los datos introducidos son falsos, dio lugar a que en el Proyecto de ley orgánica por el que se modifica el Código penal, de 27 de noviembre de 2009, se incluyera una nueva redacción del apartado segundo del art. 248 CP, con una letra c) que considera reos de estafa a «los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en ellos, realicen operaciones de cualquier clase en perjuicio de su titular»[88].

Con esta interpretación de lo que se entiende por manipulación informática, que incluye la introducción de los datos del verdadero titular en el sistema, sin contar con su autorización, para realizar una transferencia patrimonial, esto es, la suplantación de identidad en el comercio electrónico o en los cajeros automáticos, sin autorización del titular, para obtener bienes cuyo pago se carga en la cuenta del ti-

[87] Como ocurre en el «*pharming*». Cfr. FERNÁNDEZ TERUELO, J. G., «Respuesta penal», cit., p. 233-234.

[88] VALLE MUÑIZ, J. M., *El delito de estafa. Delimitación jurídico penal con el fraude civil*, Bosch, Barcelona, 1987, p. 208.

tular o para extraer dinero del cajero automático puede ser considerada estafa informática[89].

> Se trata de un fenómeno sumamente extendido, si bien en algún estudio se apunta que sólo en el 11.7% de los casos de fraude en el comercio electrónico se utilizaron datos de identidad reales. En el resto de los casos se emplearon identidades falsas (las ya mencionadas «*synthetic identities*») o bien una mezcla de datos reales y falsos[90].

En relación a la manipulación de tarjetas de crédito o de débito en el tráfico económico, es estafa informática aparentar ser el titular legítimo de una tarjeta cuya banda magnética o chip han sido manipulados o copiados, o a cuyos datos se ha accedido ilícitamente, de forma que los gastos causados en operaciones de comercio electrónico se cargan a la cuenta del titular, sin su consentimiento, causándole un perjuicio a él o a otra persona[91].

La utilización de una tarjeta perdida por el titular u obtenida por un medio constitutivo de infracción penal (por ej., una falsificación) para extraer dinero de un cajero automático es estafa informática, al

---

[89] Apunta MATA Y MARTÍN, R. M., *Estafa convencional*, cit., p. 79, nota núm.47, que «esto implica... el refuerzo de la tesis —mantenida ya generalmente por los Tribunales— de que la utilización fraudulenta de los datos de una tarjeta que atribuían falsamente el pago de una operación al titular, resultaba punible como delito de estafa, pese a las dudas suscitadas por alguna resolución judicial».

[90] En contra de la subsunción de estos casos en el concepto de manipulación informática o artificio semejante, entre otros, BAJO FERNÁNDEZ, M., «Artículo 248», en COBO DEL ROSAL, M. (Dir.), *Comentarios al Código penal. Tomo VIII. Delitos contra el patrimonio y contra el orden socioeconómico. Artículos 234 a 272*, EDERSA, Madrid, 2005, p. 298; CHOCLÁN MONTALVO, J. A., «Fraude informático», cit., pp. 345-346; FERNÁNDEZ GARCÍA, E. M., «Los fraudes», cit., pp. 141-142 y 147-148, si bien en la p. 149 parece admitir que se incluyan en el concepto de artificio semejante; FERNÁNDEZ TERUELO, J. G., *Cibercrimen*, cit., pp. 47 y 51-52; RUIZ RODRÍGUEZ, L. R., «Uso ilícito», cit., pp. 8-9; VILLACAMPA ESTIARTE, C., «La falsificación», cit., p. 5, que sólo admite la estafa informática si la tarjeta ha sido falsificada. Vid. a favor la STS de 24-2-2006 (RJ 2006\5794), que absuelve, pero afirma que «el uso abusivo de tarjetas que permiten operar en un cajero automático puede ser actualmente subsumido en el 248.2 (la estafa informática), dado que tal uso abusivo constituye un artificio semejante a una manipulación informática, pues permite lograr un funcionamiento del aparato informático contrario al fin de sus programadores»; también a favor la STS de 9-5-2007 (RJ 2007\3577), que señala que «la identificación a través del número secreto genera una presunción de uso del sistema por parte de su titular, y por ello, debe incluirse como una modalidad de manipulación informática, a los efectos de aplicar el art. 248.2 CP, el mero hecho de utilizar el número secreto de otro para identificarse ante el sistema, aunque incluso dicho número hubiera sido obtenido al margen de cualquier actividad delictiva».

[91] Cfr. el estudio, presentado en febrero de 2007, de ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf [Fecha de consulta: 9/10/09], p. 3.

existir manipulación del sistema informático en el sentido que hemos recogido en su momento, pues se utilizan los datos reales del verdadero titular, sin su consentimiento[92].

El empleo de la coletilla final «u otro artificio semejante», aunque no es una técnica desconocida en el Código penal, suscita dudas en cuanto a que respete en la medida apropiada el principio de taxatividad, y relacionado con él, el de legalidad[93]. La única forma de reducir la excesiva extensión de la conducta típica consiste en entender que el artificio, que por exigencia legal debe ser semejante a la manipulación informática, ha de suponer el empleo de tecnología avanzada[94], necesariamente informática.

---

[92] Vid. la STS de 20-11-2001 (RJ 2002\805). En la jurisprudencia menor, la SAP de Málaga de 25-6-2005 (ARP 2005\19). Así, es estafa informática el caso de la SAP de Cantabria de 26-7-2000 (JUR 2000\288359), en el que los autores, fingiendo tener un negocio, consiguen de la entidad bancaria la entrega de un terminal de punto de venta, que utilizan para realizar cargos en tarjetas cuyos números habían obtenido sin que se sepa cómo, sin consentimiento de los titulares. Un supuesto de hecho similar se encuentra en la STS de 26-6-2006 (RJ 2006\4925), siendo la única diferencia que en ésta el restaurante tenía actividad. En estos casos la transacción es electrónica y hay manipulación informática, pues aunque los datos introducidos son correctos y el sistema funciona adecuadamente se consigue la transferencia de un activo patrimonial suplantando en el sistema la identidad de los titulares legítimos de los datos. En contra, vid. RODRÍGUEZ MOURULLO, G./ALONSO GALLO, J./LASCURAÍN SÁNCHEZ, J. A., «Derecho Penal e Internet», en CREMADES, J./FERNÁNDEZ-ORDÓÑEZ, M. A./ILLESCAS, R. (Coords.), *Régimen jurídico de Internet*, La Ley, Madrid, 2002, p. 291, que aplican a estos supuestos la estafa común.

[93] A favor, vid. la STS de 20-11-2001 (RJ 2002\805), que entiende que «la conducta de quien aparenta ser titular de una tarjeta de crédito cuya posesión detenta de forma ilegítima y actúa en connivencia con quien introduce los datos en una máquina posibilitando que ésta actúe mecánicamente está empleando un artificio para aparecer como su titular ante el terminal bancario a quien suministra los datos requeridos para la obtención de fondos de forma no consentida por el perjudicado». En contra de la calificación como estafa informática, vid. las SSTS de 16-3-1999 (RJ 1999\1442) y 29-4-1999 (RJ 1999\4127). En la doctrina, también en contra, vid. BAJO FERNÁNDEZ, M., «Artículo 248», cit., p. 298; BOLEA BARDÓN, C./ROBLES PLANAS, R., «La utilización de tarjetas ajenas en cajeros automáticos: ¿Robo, hurto o estafa?», *La Ley* 2001-4, p. 1448; CHOCLÁN MONTALVO, J. A., «Fraude informático», cit., pp. 344-346; FERNÁNDEZ GARCÍA, E. M./LÓPEZ MORENO, J., «La utilización indebida», cit., p. 185; RUIZ RODRÍGUEZ, L. R., «Uso ilícito», cit., p. 9; VALLE MUÑIZ/QUINTERO OLIVARES en QUINTERO OLIVARES, G. (Dir.), *Comentarios a la Parte Especial*, 7.ª ed. cit., p. 647.

[94] Así se apunta de forma prácticamente unánime en la doctrina. Vid. por todos HERRERA MORENO, M., «El fraude informático», margs. 956-958. Sin embargo, no falta quien considera que esa referencia a una fórmula genérica era «inevitable». Cfr. VALLE MUÑIZ/QUINTERO OLIVARES en QUINTERO OLIVARES, G. (Dir.), *Comentarios a la Parte Especial*, 7.ª ed. cit., p. 649.

> El artificio ha de ser semejante a la manipulación informática, esto es, la expresión utilizada por el legislador debe entenderse en el sentido de un «artificio informático semejante», y no en el sentido de un «artificio no informático semejante»[95].
>
> En la jurisprudencia se encuentra algún caso en que se aplica la estafa informática por artificio semejante a supuestos de utilización abusiva de una tarjeta que debía entregarse a su titular, en el comercio tradicional, en connivencia con el comerciante y en perjuicio del titular[96]. Este supuesto se diferencia del «*carding*», que hemos visto anteriormente, por el hecho de que aquí no existe el engaño que ocasiona el error que produce el desplazamiento patrimonial, por lo que no es aplicable la estafa común. Tampoco resulta engañado el titular de la tarjeta, que simplemente desconoce su utilización, ni el comerciante, con el que el delincuente actuaba de común acuerdo. A mi juicio se trata, en efecto, de estafa informática, pero no por artificio semejante, sino directamente por manipulación informática: se suplanta la identidad del verdadero titular en el sistema.

En cualquier caso, la gran amplitud de la figura delictiva que nos ocupa obliga a efectuar una cuidadosa interpretación de los elementos típicos para no extender su aplicación en exceso. Con el fin de distinguir adecuadamente la estafa informática de otras conductas que pueden ser abarcadas perfectamente por los delitos de estafa común, hurto, robo con fuerza en las cosas, apropiación indebida, falsedad documental o falsificación de moneda, hay que poner de manifiesto que lo relevante no es que la transferencia de activos patrimoniales se produzca por medios informáticos, ni que se utilicen medios infor-

---

[95] Así, destacando la importancia de que se exija una semejanza entre los artificios y las manipulaciones informáticas, MATA Y MARTÍN, R. M., *Delincuencia informática*, cit., pp. 48-49. Vid. también ANARTE BORRALLO, E., «Incidencia», cit., p. 233. Afirma que con la expresión «artificio semejante» se hace referencia a la manipulación de «soportes electrónicos o telemáticos», SUÁREZ GONZÁLEZ en RODRÍGUEZ MOURULLO, G. (Dir.), *Comentarios*, cit., p. 711; añaden a éstos los ficheros informáticos, electrónicos o telemáticos y los soportes informáticos VIVES ANTÓN/GONZÁLEZ CUSSAC en VIVES ANTÓN, T. S. (Coord.), *Comentarios, II*, cit., p. 1238.

[96] Sobre esta disyuntiva, vid. GALÁN MUÑOZ, A., *El fraude*, cit., p. 566. A favor de la posición que se adopta en el texto, vid. BAJO FERNÁNDEZ, M., «Artículo 248», cit., pp. 294-295, que afirma que el artificio semejante «debe de contener algún elemento informático para entender cumplido el principio de legalidad excluyente de la analogía en la interpretación y redacción de los tipos»; MAGALDI PATERNOSTRO en CÓRDOBA RODA, J./GARCÍA ARÁN, M. (Dirs.), *Comentarios, I*, cit., p. 771 a quien parece «semántica y lógicamente plausible» vincular el artificio semejante a la expresión típica de manipulación informática; MATA Y MARTÍN, R. M., *Estafa convencional*, cit., p. 94, que alega que «la semejanza reclamada por el precepto apunta necesariamente a la calificación como informático tanto de la manipulación como del artificio»; QUERALT JIMÉNEZ, J. J., *Parte especial*, 5.ª ed. cit., p. 481, para quien el artificio análogo «es una variante de la alteración informática».

máticos para encubrir apoderamientos o disposiciones efectuados por otros medios[97], sino que la manipulación realizada por el autor[98] y que lleva a esa transferencia no consentida tenga lugar a través de sistemas informáticos.

El resultado de la manipulación informática o artificio semejante ha de ser la transferencia no consentida de un activo patrimonial en perjuicio de tercero. La transferencia constituye un resultado material intermedio que puede no significar todavía la lesión del bien jurídico si no implica simultáneamente el perjuicio de tercero. Por transferencia de un activo patrimonial se ha de entender el traspaso fáctico de un activo, es decir, de un elemento patrimonial valorable económicamente, de un patrimonio a otro[99], traspaso que no necesariamente tiene que producirse por medios electrónicos[100], aunque, dada la naturaleza del delito, ésta sea la forma más habitual. Tampoco el activo patrimonial tiene que estar obligatoriamente representado mediante anotaciones o registros informáticos[101], aunque esta modalidad esté incluida en el concepto. Se ha planteado el problema de si la obtención de servicios puede considerarse una transferencia no consentida de activos patrimoniales.

> En la jurisprudencia se ha negado que usar un cupón de abono del que no se es titular por un torniquete para conseguir el acceso y realizar el viaje sea una manipulación informática, al estimar que falta la transferencia del activo patrimonial[102], tesis con la que coincide la

[97] Cfr. STS de 20-11-2001 (RJ 2002\805).

[98] Lo advierten, entre otros, GONZÁLEZ RUS, J. J., «Protección penal», III.1; y MATA Y MARTÍN, R. M., *Estafa convencional*, cit., pp. 71 ss; del mismo autor, «Medios electrónicos de pago», cit., pp. 347-348.

[99] Así, por ej., el aprovechamiento de un fallo informático existente en algunos cajeros, de forma que encadenando una operación de solicitud de saldo con otra de reintegro en ocasiones no se pedía autorización de pago, facilitando el dinero (supuesto de hecho de la SAP de Granada de 26-9-2002, ARP 2002\273683, que castiga por estafa informática), no es manipulación informática ni artificio semejante, pues no se manipula el sistema, que es de por sí defectuoso.

[100] En este sentido, que se puede considerar amplio, vid. PÉREZ MANZANO en BAJO FERNÁNDEZ, M. (Dir.), *Compendio (Parte Especial), II*, cit., pp. 456-457.

[101] Como dan a entender, entre otros, GONZÁLEZ RUS, J. J., «Protección penal», III.1, o MATA Y MARTÍN, R. M., «Criminalidad Informática», cit., p. 217. De acuerdo con la novena acepción del término «activo» en el Diccionario de la Lengua Española, se trata del «*Econ.* Conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo, y que se reflejan en su contabilidad».

[102] Como afirman GALÁN MUÑOZ, A., *El fraude*, cit., p. 613, o MATA Y MARTÍN, R. M., «Criminalidad Informática: una introducción al cibercrimen», en RUIZ MIGUEL, C., y otros, *Temas de Direito da Informática e da Internet*, Coimbra Editora, Coimbra, 2004, p. 217, entre otros.

Fiscalía General del Estado cuando niega que el disfrute de un servicio sin abonar la contraprestación correspondiente suponga transferencia de un activo patrimonial[103]. Sin embargo, en otras ocasiones se admite la existencia de transferencia cuando lo que hay es la obtención de un servicio sin abonar su importe, previa manipulación de los códigos de acceso a la televisión de pago[104]. La doctrina y otro sector jurisprudencial afirman que también la obtención de un servicio sin el abono de su importe, siempre que se utilice una manipulación informática o artificio semejante (lo que incluye, entre otros supuestos, la suplantación de identidad[105]), supone la transferencia de un activo patrimonial que da lugar a la aplicación del delito que nos ocupa[106]. A nuestros efectos, lo que interesa resaltar es que se señala que «aunque ciertamente tal manipulación no produce la transferencia inmediata de efectivo metálico o de valores que lo representen..., en la medida en que lo que ha hecho es confeccionar una especie de llave falsa, a modo de artificio semejante, que ha permitido al agente la obtención de un servicio sin el correlativo abono de su importe y ello, en cuanto comportó y generó un perjuicio para la sociedad de telecomunicaciones, uno de cuyos activos patrimoniales precisamente es el precio de los servicios que oferta —además de los derechos por la utilización sin

---

[103] SAP de Madrid de 21-4-1999 (ARP 1999\2047).

[104] Se analizaba el supuesto de manipulación de tarjetas prepago para realizar llamadas telefónicas sin abonar la contraprestación correspondiente, concluyendo la Fiscalía que «una vez finalizada la operación y agotada la prestación del servicio no se puede decir que el patrimonio del sujeto activo se haya visto incrementado». Consulta 3/2001, de 10 de mayo, sobre la calificación jurídico-penal de la utilización, en las cabinas públicas de teléfonos, de instrumentos electrónicos que imitan el funcionamiento de las legítimas tarjetas prepago, apartado V. En el apartado VI se defiende la incardinación de esta conducta en el art. 255.1 o 3 CP, que castiga con la pena de multa de tres a doce meses las defraudaciones de fluido eléctrico y análogas por valor superior a 400 euros, o en el art. 623.4 CP, en caso de no superar ese valor.

[105] Así, la SAP de Baleares de 18-1-2006 (JUR 2006\120807), donde se señala que «aunque ciertamente tal manipulación no produce la transferencia inmediata de efectivo metálico o de valores que lo representen, como ocurre con las operaciones bancadas o de entrega de numerario en supuestos de utilización en cajeros automáticos de tarjetas falsas y no son las legítimas sustraídas a sus titulares, o cuando a través de manipulaciones de asientos contables se consiguen traspasos de efectivo o desaparición de saldos deudores, en la medida en que lo que ha hecho es confeccionar una especie de llave falsa, a modo de artificio semejante, que ha permitido al agente la obtención de un servicio sin el correlativo abono de su importe y ello, en cuanto comportó y generó un perjuicio para la sociedad de telecomunicaciones, uno de cuyos activos patrimoniales precisamente es el precio de los servicios que oferta - además de los derechos por la utilización sin su permiso de programas informáticos, debe ser equivalente a la transferencia de un activo patrimonial». En mi opinión, es evidente que con esta interpretación se roza la analogía «*in malam partem*».

[106] En contra, la SAP de Madrid de 21-4-1999 (ARP 1999\2047), ya citada, que afirma que pasar con un cupón de abono del que no se es titular por el torniquete de entrada no supone manipulación informática, sin contemplar la posibilidad de acudir al artificio semejante.

> su permiso de programas informáticos—, debe ser equivalente a la transferencia de un activo patrimonial». En mi opinión, y como ya apunté anteriormente, resulta evidente que se acoge una interpretación analógica contraria al reo, pese a reconocerse paladinamente que la manipulación no produce la transferencia de un activo patrimonial, como exige el tipo.

Además, el autor de la manipulación informática debe actuar en perjuicio de tercero, lo que se interpreta como el resultado del delito, elemento coincidente en la estafa común y en la informática. Sólo la causación efectiva del perjuicio como consecuencia de la transferencia no consentida de activos patrimoniales, conseguida a través de una manipulación informática o artificio semejante, da lugar a la consumación[107].

> A veces una mera anotación contable ya puede suponer ese perjuicio, dando lugar a la consumación del delito[108].

El hecho de que el tercero, por ej., el titular de la tarjeta o cuenta bancaria objeto del ataque, debido a las relaciones contractuales existentes con otros sujetos, consiga finalmente que su patrimonio no se vea afectado no impide la aplicación del precepto, pues lo que ocurre simplemente es que el perjuicio se traslada a otro sujeto, sin desaparecer.

También coinciden los dos primeros apartados del art. 248 CP en la exigencia de ánimo de lucro, que lleva implícita la de dolo directo, de forma que no se da el elemento subjetivo necesario en este delito cuando el objetivo del autor no es conseguir la transferencia de activos en perjuicio de otro, sino otro propósito[109].

El perjuicio causado debe ser superior a 400 euros[110]. Si se causa un perjuicio inferior a 400 euros se acude a la falta del art. 623.4 CP,

---

[107] Cfr. CHOCLÁN MONTALVO, J. A., «Infracciones patrimoniales», cit., pp. 255-256; RODRÍGUEZ MOURULLO, G./ALONSO GALLO, J./LASCURAÍN SÁNCHEZ, J. A., «Derecho Penal e Internet», cit., pp. 290-291; ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Comares, Granada, 2002, p. 579.

[108] Vid. ampliamente, MATA Y MARTÍN, R. M., *Estafa convencional*, cit., pp. 103 ss. No es suficiente que se ocasione un peligro para el patrimonio, pues es necesario el perjuicio efectivo. Critica que no se haya optado por limitarse a una descripción detallada de las acciones típicas, configurándose la estafa informática como un tipo de peligro y no de lesión, LÓPEZ BARJA DE QUIROGA, J., «El moderno derecho penal para una sociedad de riesgos», *Revista del Poder Judicial* núm.48, 1997, p. 306.

Tampoco basta para la consumación con que se obtenga un beneficio si con ello no se ha perjudicado a nadie. Cfr. ANARTE BORRALLO, E., «Incidencia», cit., p. 236.

[109] En contra, ANARTE BORRALLO, E., «Incidencia», cit., p. 236.

[110] Cfr. ANARTE BORRALLO, E., «Incidencia», cit., p. 237.

que sanciona a «los que cometan estafa..., en cuantía no superior a 400 euros», con la pena de localización permanente de cuatro a doce días o multa de uno a dos meses[111].

> A ello no se opone el que hayamos hablado antes de que la estafa informática sea una figura autónoma frente a la estafa común, pues esta afirmación se limita a poner de relieve que no se pueden exigir los elementos típicos característicos de la estafa común. Ahora bien, la estafa informática se regula en la Sección 1.ª, «De las estafas», del Capítulo VI, «De las defraudaciones», del Título XIII. A estos efectos es una estafa, si bien carece de la estructura de la común.

En conclusión, el delito de estafa informática permite abarcar los casos de usurpación de la identidad de otro en el comercio electrónico sin su consentimiento.

IV. Posibilidades y límites de los delitos de falsedad

1. Determinaciones previas

Los delitos de falsedad plantean una problemática muy interesante en el marco de la suplantación de identidad, pues cuando se produce la exhibición de un documento de identidad auténtico perteneciente a otra persona o falsificado para reforzar el engaño puede producirse un concurso de delitos. Además, la extraordinaria protección que reciben las tarjetas, equiparadas a la moneda a efectos del delito de falsificación de moneda, obliga a analizar también esta figura delictiva en los casos en que lo que hay es una falsificación de este objeto material.

---

[111] En este sentido, exigiendo el perjuicio superior a 400 euros para aplicar el delito de estafa informática, CHOCLÁN MONTALVO, J. A., «Fraude informático», cit., p. 338. En contra, por todos, HERRERA MORENO, M., «El fraude informático», marg. 961, que sostiene que al no ser el fraude informático una estafa, la causación de un perjuicio inferior a lo dispuesto en el Código penal quedaría impune, al no poder aplicarse la falta. También en contra, MATA Y MARTÍN, R. M., *Estafa convencional*, cit., p. 107, que reconoce que la exigencia de una cuantía mínima para aplicar el delito de estafa informática carece de apoyo legal, pero entiende que ello supone una analogía favorable al reo, no siendo posible acudir a la falta de estafa «al no establecer el tipo ninguna conexión con la manipulación y dado que se ha entendido necesario incorporar tal elemento para salvar su incompatibilidad con la formulación tradicional».

2. *Falsedad documental*

La presentación de un documento de identidad, sea material o electrónico, auténtico pero perteneciente a otra persona para hacerse pasar por ella en el tráfico jurídico-económico no recibe sanción en nuestro Ordenamiento jurídico. En efecto, aunque podría plantearse la aplicación de alguno de los delitos contenidos en el Título XVIII del Libro II del Código Penal, «De las falsedades», en concurso con alguna de las modalidades de estafa, dicha posibilidad es rechazada mayoritariamente por la doctrina.

> El documento de identidad electrónico encaja en el concepto de documento que se utiliza en el art. 24 CP. Aún así, no son aplicables los delitos de falsedad documental porque no se falsifica un documento o certificado ni se usa un documento o certificado manipulado o falso, sino uno auténtico. En la doctrina se descarta también la aplicación del delito de usurpación del estado civil (art. 401 CP), «tanto por su formal desconexión de lo documental como por que la orientación del delito a la usurpación del estado civil lo aleja definitivamente de unas conductas en las que no se pretende eso sino simplemente engañar a otras personas sobre algún extremo que es de obligado cumplimiento para conseguir algo sometido a alguna clase de control reglamentario o contractual»[112]. Y en cualquier caso se suele afirmar que de concurrir la usurpación de estado civil con una estafa el concurso es de infracciones[113].
>
> Consciente de esta laguna, el legislador, en el Proyecto de ley de modificación del Código penal, de 27 de noviembre de 2009, propone introducir un nuevo art. 400 *bis* del siguiente tenor: «En los supuestos descritos en los artículos 392, 393, 394, 396 y 399 de este Código también se entenderá por uso de documento, despacho, certificación o documento de identidad falsos el uso de los correspondientes documentos, despacho, certificación o documento de identidad auténticos realizado por quien no esté legitimado para ello».

Cuestión distinta es que se utilice un documento de identidad previamente falsificado por un tercero, pues en este caso puede haber delito de uso de documento falso (art. 393, normalmente en rela-

---

[112] En contra, por todos, QUERALT JIMÉNEZ, J. J., *Parte especial*, 5.ª ed. cit., p. 481, por entender que en realidad «seguimos sin estar ante una estafa».

[113] QUINTERO OLIVARES, G., «Fraudes», cit., p. 101, que propone introducir una modalidad de falsedad que extienda la sanción «a quienes utilicen en sus relaciones con la Administración o jurídicas con otras personas documentos o certificados que no le pertenezcan, prescindiendo de que eso se hiciera con o sin el consentimiento del titular» (pp. 101-102).

ción con el art. 392 CP)[114]. Aquí ha de tenerse en cuenta que el uso de documentos de identidad falsificados en el extranjero no se considera, por regla general, una conducta típica en España, conforme al acuerdo del Pleno no Jurisdiccional de la Sala Segunda del Tribunal Supremo de 27 de marzo de 1998, que recoge la salvedad de que los documentos se presenten en juicio o se usen para perjudicar a tercero, o que esas falsificaciones afecten a los intereses del Estado. Cuando los documentos de identidad falsos son aprehendidos en nuestro país, sin embargo, se entiende que tal conducta afecta a los intereses del Estado, conforme a lo previsto en el art. 23.3 f) LOPJ, que dispone que corresponde a la jurisdicción española el conocimiento de los hechos cometidos por españoles o extranjeros fuera del territorio nacional cuando se trate de delitos de falsificación que perjudiquen directamente el crédito o los intereses del Estado[115].

> Para cubrir mejor estos supuestos, el Proyecto de ley de modificación del Código penal, de 27 de noviembre de 2009, inclue varias modificaciones en el art. 392 CP, cuyo texto pasaba a ser el siguiente: «La misma pena (de la falsedad en documento público, oficial o mercantil cometida por particular) se impondrá al que hiciere uso, a sabiendas, de un documento de identidad falso así como al que sin haber intervenido en su falsificación traficare con él de cualquier modo. Esta disposición es aplicable aun cuando el documento de identidad falso aparezca como perteneciente a otro Estado de la Unión Europea o a un tercer Estado o haya sido falsificado o adquirido en otro Estado de la Unión Europea o en un tercer Estado si es utilizado en España». En la exposición de motivos se apuntaba que «como novedad importante debe destacarse que se podrá considerar falsedad también el uso de documento, despacho, certificación o documento de identidad falsos, por quien no esté legitimado para ello, con independencia del modo en que haya conseguido el documento, pues es evidente que la infracción no puede depender del consentimiento de otra persona siendo el bien jurídico afectado de carácter claramente supraindividual».

Si el documento de identidad ha sido falsificado por la misma persona que posteriormente realiza una estafa cuyo engaño se basa en la suplantación de identidad, nos encontramos ante un concurso medial de delitos entre la falsedad en documento oficial y esta figura[116], nuevamente con la prevención de que el art. 23.3 LOPJ

---

[114] ORTS BERENGUER en VIVES ANTÓN, T. S., y otros, *Parte Especial*, 2.ª ed. cit., p. 654.

[115] Cfr. FERNÁNDEZ ENTRALGO, J., «Falsificación», cit., p. 59; ROMEO CASABONA, C. M., «Delitos», cit., p. 113.

[116] Es postura jurisprudencial ya consolidada la relativa a que tales falsificaciones de documentos de identidad, en cualquier lugar que sean perpetradas, afectan direc-

sólo faculta a los tribunales españoles para conocer de las falsificaciones cometidas por españoles o por extranjeros en el extranjero cuando dichas falsificaciones perjudiquen los intereses del Estado[117].

Así pues, mientras no se produzca una reforma del Código penal, el delito de falsificación en documento oficial extranjero cometido en el extranjero, fuera de los casos en que se ocasionan perjuicios al Estado, no es perseguible en España, donde también se considera atípico el uso de tal documento. Fuera de estos supuestos, se aplica un concurso medial entre falsedad en documento oficial por particular y estafa.

> En este caso, es más grave el delito de falsedad en documento oficial por particular (castigado con penas de prisión de seis meses a tres años y multa de seis a doce meses) que la estafa (castigada con pena de prisión de seis meses a tres años). La mitad superior de la pena que corresponde imponer al delito más grave es prisión de un año, nueve meses y un día a tres años y multa de nueve meses y un día a doce meses.

3. Falsificación de moneda

La manipulación de tarjetas presenta una interesante problemática añadida. Estando en vigor el Código penal de 1944, ante la falta de una regulación expresa de la falsificación de tarjetas y en vista de que la tarjeta podía ser considerada documento mercantil, se estimó que su falsificación constituía delito de falsedad en documento mercantil[118]. Planteaba problemas el supuesto de exclusiva manipulación de la banda magnética, siendo su consideración como documento mercantil mucho más discutida, debido a que, aunque

---

tamente a los intereses del Estado. Así se recoge en las SSTS de 20-1-2004 (RJ 2004\7531), 5-4-2006 (RJ 2006\2288), 11-4-2006 (RJ 2006\2266) y 25-1-2007 (RJ 2007\1171), argumentándose al efecto que dejaría mucho que desear el crédito que el Estado tiene ante sus propios ciudadanos y ante la opinión internacional si no es capaz de poner los medios para identificar a quienes se encuentran en su territorio o pretenden llegar al mismo a través de sus fronteras.

[117] El uso del documento falso por el falsificador no es más que el agotamiento material del delito de falsedad documental, según posición unánime de doctrina y jurisprudencia.

[118] La falta de competencia de los tribunales españoles para conocer de las falsedades cometidas sobre documentos extranjeros en el extranjero ha sido reconocida, entre otras resoluciones, en la STS de 18-6-1999 (RJ 1999\5656) y en la SAP de Navarra de 28-10-2002 (JUR 2003\12502).

contiene datos con capacidad para probar hechos con trascendencia jurídica, dichos datos no son legibles directamente[119].

En la actualidad, tras la entrada en vigor del Código penal de 1995, las diversas conductas relacionadas con la falsificación de tarjetas de crédito o de débito, o que puedan usarse como medios de pago, se castigan como delito de falsificación de moneda por expresa determinación legal. En efecto, de acuerdo con lo dispuesto en el art. 386 CP, «será castigado con la pena de prisión de ocho a 12 años y multa del tanto al décuplo del valor aparente de la moneda[120]: 1º El que altere la moneda o fabrique moneda falsa. 2º El que introduzca en el país o exporte moneda alterada. 3º El que transporte, expenda o distribuya, en connivencia con el falsificador, alterador, introductor o exportador, moneda falsa o alterada». Se impone la pena inferior en uno o dos grados, atendiendo al valor de la moneda falsa y al grado de connivencia con los autores mencionados en los números anteriores, la tenencia para su expendición o distribución, así como la adquisición, sabiéndola falsa, con el fin de ponerla en circulación. El último inciso del precepto contempla un subtipo agravado por pertenencia del culpable «a una sociedad, organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de estas actividades», pudiéndose imponer en tal caso «alguna o algunas de las consecuencias previstas en el artículo 129 de este Código»[121]. Por su parte, el art. 387 CP señala que «a los efectos del artículo an-

[119] Así, las SSTS de 19-6-1986 (RJ 1986\3176), en relación a las tarjetas de compra de grandes almacenes, de 16-7-1987 (RJ 1987\5541), ya en relación a tarjetas de crédito, de 10-6-1991 (RJ 1991\4556), relativa al talón de venta realizada con tarjeta de crédito, de 3-12-1991 (RJ 1991\8955) y de 15-3-1994 (RJ 1994\2317), entre otras. No cabe duda que las tarjetas son documentos mercantiles.

[120] En la jurisprudencia se encuentran resoluciones que aplican el delito de falsedad documental a casos de manipulación de la banda magnética. Así, la STS de 11-7-2001 (RJ 2001\6377). Ponía en duda que la banda magnética pudiera ser considerada documento a efectos penales, bajo la vigencia del Código penal de 1944/73, ROMEO CASABONA, C. M., *Poder informático*, cit., pp. 79 ss; del mismo autor, «Delitos», cit., p. 127. Vid. también GONZÁLEZ RUS, J. J., «Tratamiento penal», cit., p. 51, que posteriormente ha cambiado de opinión (por ej., vid. «Protección penal», III.2.C).

[121] Tratándose de falsificación de tarjetas, el Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo de 28 de junio de 2002 acordó que, en los casos de manipulación de la banda magnética, dada la imposibilidad de determinación del «valor aparente» de lo falsificado, no procede aplicar la pena de multa. Muy crítico con esta decisión, por entender que se crea una pena ilegal al mutilar la que prevé el Código penal, QUERALT JIMÉNEZ, J. J., *Parte especial*, 5.ª ed. cit., p. 670, que propone, para «salvar este escollo y ser respetuoso con el principio de legalidad... castigar la falsificación la tarjeta de crédito o débito cuya banda magnética de modo que no incluya límite de disposición o de cargo con el más límite más alto que exista en el mercado» (sic), lo que a mi juicio es inadmisible.

terior... se considerarán moneda las tarjetas de crédito, las de débito y las demás tarjetas que puedan utilizarse como medio de pago...». Esta enumeración plantea varios problemas, desde saber qué tarjetas son de crédito o débito, hasta delimitar cuáles son esas otras que, sin ser de crédito o débito, pueden utilizarse como medio de pago. A mi juicio, resulta aplicable la definición de «instrumento de pago» que se contiene en la Decisión marco 2001/413/JAI del Consejo, de acuerdo con la cual «a efectos de la presente Decisión marco, se entenderá por: a) «instrumento de pago»: todo instrumento material, exceptuada la moneda de curso legal (es decir los billetes de banco y las monedas metálicas), que por su naturaleza específica permita, por sí solo o junto con otro instrumento (de pago), al titular o usuario transferir dinero o un valor monetario - como, por ejemplo, tarjetas de crédito, tarjetas eurocheque, otras tarjetas emitidas por entidades financieras, cheques de viaje, eurocheques, otros cheques o letras de cambio - que esté protegido contra las imitaciones o la utilización fraudulenta, por ejemplo, a través del diseño, un código o una firma». Atendiendo a esta definición, además de las tarjetas de crédito o de débito emitidas por entidades financieras, debe castigarse como falsificación de moneda la falsificación del soporte material de las tarjetas prepago, incluidos los monederos electrónicos[122].

> También denominadas tarjetas inteligentes («*smart cards*») o tarjetas chip, las tarjetas monedero han sido desarrolladas como alternativa a los micropagos. La idea consiste en utilizarlas como monederos digitales, poseyendo las características más relevantes de un monedero real, pero, presumiblemente, sin sus inconvenientes. Al igual que un monedero común, el electrónico permite almacenar una cantidad variable de dinero, en general no muy elevada; el proceso de pago es rápido y sencillo; los pagos son anónimos, ya que a partir del dinero recibido no se puede rastrear al pagador; el dinero es aceptado en cualquier parte del país, por cualquier comerciante. El monedero electrónico consiste en una tarjeta que incorpora un pequeño chip en el que se almacena un valor monetario prepagado, que puede ser gastado en cualquier comercio que haya instalado un lector de tales tarjetas. Sin entrar en la discusión acerca de si estas tarjetas son o no tarjetas de crédito o de débito, a mi juicio no cabe duda de que sirven como medio de pago[123], como las califican las propias entidades financieras y de crédito que la promocionan.

---

[122] En la doctrina se criticaba la falta de previsión de un subtipo agravado cuando el delito era cometido en el seno de una organización delictiva. Cfr. ARÁNGUEZ SÁNCHEZ, C., *La falsificación de moneda*, Bosch, Barcelona, 2000, p. 104.

[123] Pero no las tarjetas virtuales o cibertarjetas, proporcionadas por algunas entidades financieras, que se componen de un número, un PIN y una fecha de caducidad, sin soporte físico, y sólo se utilizan para transacciones en Internet. Este tipo de tarjeta

La cuestión es más discutida en relación a las tarjetas prepago que sirven a una única función, normalmente como título que legitima a la prestación de un servicio, como las tarjetas de Telefónica[124]. No están personalizadas, de forma que su utilización indebida por quien no la ha adquirido lícitamente no supone suplantación de identidad.

> La Consulta 3/2001, de 10 de mayo, de la Fiscalía General del Estado, responde a la cuestión relativa a si las tarjetas prepago de la compañía Telefónica son o no tarjetas de crédito o de débito, descartando que su manipulación pueda considerarse falsificación de moneda por no encajar en estos conceptos: «la respuesta ha de ser, coincidiendo con la opinión de la Fiscalía consultante, necesariamente negativa, ya que la emisión de la tarjeta (ya sea de crédito o de débito) se basa en ambos casos en la existencia de un contrato subyacente, muy distinto de aquel en virtud del cual se adquiere una tarjeta prepago. En el caso de la tarjeta de crédito, el emisor de la tarjeta concede un crédito a su titular que le permite disponer en sus pagos hasta un determinado límite sin necesidad de anticipar el dinero, lo que obviamente no sucede en la tarjeta prepago, que como su propio nombre indica se obtiene previo pago de la cantidad de dinero correspondiente. En el caso de la tarjeta de débito, el emisor de la tarjeta permite al titular realizar una serie de pagos con cargo a un depósito de dinero previamente constituido (por lo general una cuenta bancaria) y hasta el límite de dinero disponible en dicho depósito en cada momento, lo que tampoco sucede en la adquisición de la tarjeta de Telefónica, que se obtiene mediante el pago de una cantidad que el comprador entrega en concepto de precio (por la utilización de los servicios que la compañía presta para realizar llamadas, durante un determinado tiempo y hasta el límite máximo de la cantidad entregada) y no para constituir un depósito de dinero con cargo al cual pueda ir realizando las llamadas, lo cual le permitiría entre otras cosas poder retirar del depositario la cantidad de dinero no utilizada, algo evidentemente impensable cuando se adquiere una de estas tarjetas. Además y para disipar definitivamente cualquier género de duda, hay que tener presente que tanto la tarjeta de crédito como la de débito son siempre documentos nominativos, personalísimos e

---

se basa en el prepago: el usuario carga la cantidad que desee en el cajero automático, a través de la red o en la propia entidad emisora, cuantas veces quiera. Pero al carecer de soporte material no encaja en el concepto de instrumento de pago de la Decisión marco 2001/413/JAI del Consejo, que habla de «instrumento material», y tampoco en el de documento a efectos penales, contenido en el art. 26 CP, que exige también un «soporte material». No podría ser objeto, por tanto, del delito de falsificación de moneda, que claramente presupone ese soporte material.

[124] En la doctrina, vid. entre otros, FRAMIÑÁN SANTAS, J., «Medios de pago», cit., pp. 395-396; VILLACAMPA ESTIARTE en QUINTERO OLIVARES, G. (Dir.), *Comentarios a la Parte Especial*, 7.ª ed. cit., pp. 1527-1528, que las considera tarjetas de débito.

> intransferibles, al contrario de la tarjeta prepago, que puede ser objeto de ulterior transmisión y en consecuencia utilizada por cualquier usuario, sea o no aquél a quien haya sido originalmente vendida» (Apartado II). A diferencia de las tarjeta monedero, que permiten el pago de múltiples bienes y servicios y son por lo general recargables, las tarjetas telefónicas prepagadas están limitadas a una única función y son desechables, de forma que se emiten por una cantidad fija y cuando se acaba se tiran.

De no ser consideradas medios de pago, se plantea la cuestión de cómo castigar la manipulación del chip de las tarjetas prepago de función única.

> En la Consulta 3/2001, de 10 de mayo, la Fiscalía General del Estado afirma que su alteración en elementos de carácter esencial, o su simulación en todo o en parte, pueden ser delitos de falsedad documental (Apartado III). Sin embargo, en la jurisprudencia se ha apuntado, con razón, que «la tarjeta prepago de Telefónica contiene un chip, un pequeño programa informático con unos datos que ponen en funcionamiento los teléfonos de esa Compañía y la tarjeta utilizada por la acusada emula el funcionamiento del chip de las tarjetas auténticas, consiguiendo activar el teléfono público, según se desprende del informe técnico...; pero ese programa informático no tiene otro significado ni otra finalidad que la de activar el teléfono, son unos datos materiales carentes de toda relevancia jurídica, porque no están destinados a probar nada, ni a crear constancia alguna de cara a terceros, por ello no puede integrarse el documento examinado en el concepto del art. 26 del CP, al estar ausente en el mismo el requisito normativo incluido en el precepto»[125].

En mi opinión, la falsificación de estas tarjetas prepago de función única se ha de castigar, en su caso, como delito contra la propiedad industrial. Por su parte, su utilización puede dar lugar a la aplicación del delito de defraudación de telecomunicaciones, pues el uso de una tarjeta falsificada puede ser considerado un medio clandestino empleado para realizar una defraudación que perjudica al suminis-

---

[125] A favor, vid. VILLACAMPA ESTIARTE en QUINTERO OLIVARES, G. (Dir.), *Comentarios a la Parte Especial*, 7.ª ed. cit., p. 1528, que las incluye entre las tarjetas que pueden utilizarse como medio de pago. En contra, destacando que el pago ya se ha realizado con anterioridad, sirviendo la tarjeta únicamente como título de legitimación para la entrega del bien o la prestación del servicio, ARÁNGUEZ SÁNCHEZ, C., *La falsificación de moneda*, cit., pp. 40-41, quien entiende, además, que «aun no están incluidas en el objeto material de los delitos relativos a la falsificación de moneda, por lo que su elaboración fraudulenta deberá ser considerada como una falsedad en documento mercantil». También en contra de que la falsificación de tarjetas prepago de Telefónica pueda ser considerada falsificación de moneda, ORTS BERENGUER en VIVES ANTÓN, T. S., y otros, *Parte Especial*, 2.ª ed. cit., p. 636.

trador[126] del servicio de telecomunicación[127]. Mediante un programa grabado en el chip de que disponen estos instrumentos, se proporcionan las órdenes oportunas al dispositivo del teléfono, validando los datos correspondientes como las claves y los códigos necesarios, así como la cantidad disponible durante la llamada. Dicha cantidad suele ser la máxima utilizada en las tarjetas originales a las que imitan, cantidad que el programa del chip regenera automáticamente una vez consumida, lo que permite una utilización prácticamente ilimitada de estas imitaciones en una o en múltiples llamadas. De esta forma, lo que se hace es alterar fraudulentamente las indicaciones de consumo del crédito de que dispone la tarjeta[128].

Igualmente plantea dudas la razonabilidad de extender la consideración de moneda a efectos penales a las tarjetas de compra, que permiten a su tenedor realizar compras en un establecimiento determinado, o en los establecimientos de una cadena comercial, con el compromiso de cancelar el saldo adeudado a la expiración del período de facturación, generalmente mensual. A diferencia de las bancarias, estas tarjetas no son emitidas por entidades financieras, sino por establecimientos comerciales. Sin embargo, son similares en su funcionamiento a las tarjetas de crédito o de débito diferido, en cuanto existe una concesión de crédito. Sirven, además, como instrumento o medio de pago, por lo que, en mi opinión, su falsificación debe ser castigada como de moneda.

Un sector doctrinal critica, con razón, la decisión del legislador de asimilar las tarjetas que se utilizan como medio de pago, pero son emitidas por establecimientos comerciales, a la moneda de curso le-

---

[126] SAP de Madrid de 17-10-2000 (JUR 2001\43885), FJ 1°.

[127] Algunos autores afirman que el art. 255 CP sólo sanciona el uso en beneficio propio y en perjuicio del suministrador, lo que no estimo correcto. Vid. por todos, CREMADES GARCÍA, J., «El fraude en los servicios financieros "on-line"», en AA.VV., *Estudios jurídicos. Ministerio Fiscal. II-2003. Delincuencia Informática. Drogas de abuso: Aspectos Científicos y Jurídicos. Experiencias aplicativas de la LORPM*, Ministerio de Justicia, Madrid, 2004, p. 269; GONZÁLEZ RUS, J. J., «Protección penal», II.4; MORILLAS CUEVA, L., «Artículo 255», en COBO DEL ROSAL, M. (Dir.), *Comentarios al Código penal. Tomo VIII. Delitos contra el patrimonio y contra el orden socioeconómico. Artículos 234 a 272*, EDERSA, Madrid, 2005, pp. 524-525. También lo dan así a entender VIVES ANTÓN/GONZÁLEZ CUSSAC en VIVES ANTÓN, T. S. (coord.), *Comentarios, II*, cit., p. 1269; los mismos autores en VIVES ANTÓN, T. S., y otros, *Parte Especial*, cit., p. 516. A favor de la posición recogida en el texto, vid. por todos QUERALT JIMÉNEZ, J. J., *Parte especial*, 5.ª ed. cit., p. 513.

[128] Sin embargo, para la Fiscalía General del Estado, en la Consulta 3/2001, de 10 de mayo, sobre la calificación jurídico-penal de la utilización, en las cabinas públicas de teléfonos, de instrumentos electrónicos que imitan el funcionamiento de las legítimas tarjetas prepago, encajan en el núm.1 del art. 255 CP, y para MORILLAS CUEVA, L., «Artículo 255», cit., p. 539, en el núm.3.

gal, pues claro está que no concurren las mismas razones de protección del monopolio estatal de la emisión de moneda de curso legal, lo que hace que la pena resulte excesiva[129]. Otro sector, más radical, critica también la extensión del concepto de moneda a estos efectos a las tarjetas emitidas por entidades financieras[130].

> Así, se apunta que «para que la duplicación de tarjetas sea falsificación de moneda, es preciso que, además de tratarse de una falsificación del soporte plástico, constituya, como en toda falsificación de moneda, una afectación al sistema de pagos nacional e internacional, es decir, debe crear nuevas relaciones crediticias o de débito no previstas o generadas por el sistema financiero, teniendo, por lo tanto, como fenómeno, capacidad para alterar los sistemas de pago, para generar relaciones crediticias inexistentes o débitos sobre cuentas no reales. Pero la clonación o duplicación sólo conlleva una afectación a la relación patrimonial trilateral que se crea entre el titular, el establecimiento y la entidad financiera, introduciendo a un tercero no legitimado en la misma»[131].

Ahora bien, en mi opinión, esta crítica, que está bien fundamentada[132], no puede llevar a una interpretación «*contra legem*», sino a una propuesta de modificación «*de lege ferenda*», de creación de un delito específico, en coordinación con la normativa europea, que permita tener en cuenta que estamos ante algo más que una falsificación en documento mercantil, en vista de la gravedad del desvalor que supone el atentado contra instrumentos de pago tan extendidos en la práctica comercial, pero ante algo menos que una falsificación de moneda, permitiendo captar al mismo tiempo el atentado contra el patrimonio, que de hecho queda al margen tanto en los delitos de falsedad documental como de falsificación de moneda, aunque en ambos sea necesario el propósito de introducir o usar en el tráfico económico el objeto material del delito.

> En esta dirección, el Proyecto de ley de modificación del Código penal, de 27 de noviembre de 2009, introduce una sección 4.ª en el Capí-

---

[129] Analiza un caso referido a estas tarjetas la SAP de Barcelona de 7-2-2002 (JUR 2002\124700), que absuelve por falta de prueba de que las tarjetas que habían sido ocupadas al acusado (151, todas cargadas por su importe total) hubieran sido manipuladas.

[130] Entre otros, ARÁNGUEZ SÁNCHEZ, C., *La falsificación de moneda*, cit., pp. 45-48; FERNÁNDEZ ENTRALGO, J., «Falsificación», cit., p. 50; FERNÁNDEZ GARCÍA, E. M., «Los fraudes», cit., pp. 121-122; QUINTERO OLIVARES, G., «Fraudes», cit., pp. 98-99; VILLACAMPA ESTIARTE, C., «La falsificación», cit., p. 3.

[131] Vid., entre otros, FERNÁNDEZ GARCÍA, E. M./LÓPEZ MORENO, J., «La utilización indebida», cit., p. 165; QUERALT JIMÉNEZ,J. J., *Parte especial*, 5.ª ed. cit., p. 668; VILLACAMPA ESTIARTE, C., «La falsificación», cit., p. 3.

[132] RUIZ RODRÍGUEZ, L. R., «Uso ilícito», cit., p. 5.

tulo II del Título XVIII del Libro II, con la rúbrica «De la falsificación de tarjetas de crédito y débito y cheques de viaje», donde se regulaban estas conductas en un nuevo art. 399 *bis*[133]. En la exposición de motivos se apunta que «las tarjetas de crédito o débito requieren también su propia tutela frente a la falsificación, a cuyo fin se describe específicamente esa conducta referida a ellas o a los cheques de viaje»[134].

«Nonagésimo noveno.

Se añade la Sección 4.ª del Capítulo II del Título XVIII del Libro II, que tendrá la siguiente rúbrica:

«De la falsificación de tarjetas de crédito y débito y cheques de viaje»

Centésimo.

Se añade el artículo 399 *bis*, que queda redactado como sigue:

«1. Será castigado con la pena de prisión de cuatro a ocho años el que falsificare, copiándolos o reproduciéndolos, tarjetas de crédito o débito o cheques de viaje. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o los hechos fueran cometidos en el marco de una organización criminal dedicada a estas actividades.

Los Jueces o Tribunales impondrán a la organización, bien como pena si procediere la declaración de su responsabilidad penal de acuerdo con lo dispuesto en el artículo 31 *bis* de este Código, bien como me-

[133] Vid. los argumentos que resume ARÁNGUEZ SÁNCHEZ, C., *La falsificación de moneda*, cit., pp. 45-48, siendo el más relevante, a mi juicio, que estamos hablando de títulos de carácter mercantil que no son emitidos en régimen de monopolio por el Estado, como la moneda, sino por entidades privadas, parece desproporcionada la protección que se les ofrece. Vid. no obstante la STS de 8-7-2002 (RJ 2002\8939), que en un supuesto de falsificación múltiple de tarjetas, en el que interviene una organización delictiva con conexiones en el extranjero, afirma que la pena de la falsificación de moneda, aunque elevada, «sí estaría suficientemente justificada». Otro argumento, basado en que se deja al margen el interés de la víctima, que es el titular de la tarjeta clonada o el banco que atendió el pago, empleado por QUINTERO OLIVARES, G., «Fraudes», cit., p. 96, no me parece tan relevante, puesto que el delito de falsificación de moneda sólo contempla el desvalor propio de la creación de las tarjetas, pero su empleo en el comercio debe ser sancionado a través de los delitos de estafa o estafa informática, que sí atienden al perjuicio individual.

[134] Se responde así, con cierto retraso, al pronunciamiento favorable del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo de 28 de junio de 2002, a la procedencia de que por el Tribunal competente para la resolución del recurso de casación se acudiera al Gobierno de la Nación, en aplicación de lo dispuesto en el art. 4.3 CP, exponiendo la conveniencia de la inclusión en el Código penal de un precepto específico que contemple los actos de falsificación de tarjetas, con establecimiento de las penas adecuadas para cada supuesto, en consonancia con lo previsto para esta materia en la Decisión marco 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.

dida en los casos previstos en el artículo 129, la disolución y clausura definitiva de sus locales y establecimientos.

2. La tenencia de tarjetas de crédito o débito o cheques de viaje falsificados en cantidad que permita suponer están destinados a la distribución o tráfico, será castigada con la pena señalada a la falsificación.

3. El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados será castigado con la pena de prisión de dos a cinco años».

En este precepto puede observarse que no se mencionan las demás tarjetas, al margen de las de crédito o débito, que puedan usarse como medio de pago, cuya punición tendría lugar en el marco de los delitos de falsedad en documento mercantil[135].

En cuanto a las modalidades de acción, es de resaltar que hasta la reforma operada por la LO 15/2003 se castigaba como falsificación de moneda la fabricación, esto es, la creación *ex novo* de moneda o de una tarjeta falsa imitando otra auténtica[136], pero no la alteración de moneda de curso legal o de una tarjeta legítima, conducta a la que en su día se aludía en el art. 283.2° CP 1944/73, pero que había desaparecido en la redacción del Código penal de 1995. Esta conducta resulta relevante criminológicamente no tanto en el caso de la moneda[137], cuanto de las tarjetas, que «más que ser íntegramente falsificadas, suelen ser modificadas en algunos de sus datos esenciales partiendo de un documento original, y tal conducta no puede ser encuadrada en el verbo típico «fabricar» sin forzar su sentido literal»[138]. Por este motivo, la conducta de alteración de la banda magnética de una tarjeta legítima, o de los datos del titular, la fecha de caducidad, el número, etc., contenidos en el soporte plástico de una

---

[135] Con más detalle acerca de la necesidad de prever un supuesto así, vid. QUINTERO OLIVARES, G., «Fraudes», cit., pp. 93-99.

[136] Cfr. VILLACAMPA ESTIARTE, C., «La falsificación», cit., p. 4.

[137] La modalidad de acción consisten en crear una tarjeta con datos que no se corresponden a un titular real, ni permiten su vinculación a una cuenta bancaria real, es cada vez menos frecuente, ya que la generalización de los datáfonos o terminales de punto de venta permite comprobar con carácter inmediato que la tarjeta que se entrega para el pago realmente existe, lo que hace inútil la presentación de tarjetas aparentes. Sólo se sigue empleando en casos de manipulación manual de las tarjetas. Cfr. CASTILLA CUBILLAS, M., *La tarjeta de crédito*, cit., p. 179.

[138] No obstante, no se puede descartar que se dé algún caso. Vid. la STS de 7-3-1989 (RJ 1989\2508), que entendió que el hecho de borrar con un preparado de lejía la palabra «anulado», que se había estampado sobre los billetes por la Fábrica Nacional de Moneda y Timbre para indicar que estaban destinados a su destrucción, constituía «alteración».

tarjeta legítima[139], se venía castigando en algún caso como delito de falsedad en documento mercantil, lo que daba lugar a una considerable diferencia en el trato punitivo.

> En efecto, la falsedad en documento mercantil se castiga con penas muy inferiores a las previstas para la falsificación de moneda: en el primer caso, prisión de seis meses a tres años y multa de seis a doce meses (art. 392 en relación con el art. 390.1 CP); en el segundo caso, prisión de ocho a doce años y multa del tanto al décuplo del valor aparente de la moneda (art. 386 CP).

El acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo, en su reunión de 28 de junio de 2002 (JUR 2002\192448), optó por entender que «la incorporación a la «banda magnética» de uno de estos instrumentos de pago, de unos datos obtenidos fraudulentamente, constituye un proceso de fabricación o elaboración que debe ser incardinado en el art. 386 del Código penal», poniendo fin a esta diversidad de calificaciones[140]. La misma doctrina era aplicable al supuesto en que lo que se alteraba no era una banda magnética, sino un chip electrónico. Por su parte, la reforma de la LO 15/2003 introduce como conducta típica la alteración, con lo que evita las objeciones de tipicidad que podía plantear el acuerdo del Tribunal Supremo.

> El origen de esta reforma se encuentra en el art. 1.2 del Reglamento (CE) 1338/2001 del Consejo, de 28 de junio de 2001, por el que se definen las medidas necesarias para la protección del euro contra la falsificación, que entiende por actividades de falsificación, entre otras, «todas las acciones fraudulentas de fabricación o alteración de billetes o monedas de euros, sea cual fuere el medio utilizado para producir el resultado»[141].

---

[139] ARÁNGUEZ SÁNCHEZ, C., *La falsificación de moneda*, cit., p. 51. Cfr. también VILLACAMPA ESTIARTE, C., *La falsedad documental: análisis jurídico-penal*, Cedecs, Barcelona, 1999, p. 282. Vid. no obstante la SAP de Málaga de 25-6-2005 (ARP 2005\19), FJ 2°, que sostiene que la introducción de una banda magnética nueva sobre el soporte plástico de una tarjeta legítima es fabricación, y no simplemente alteración. En sentido similar, la SAP de Madrid de 18-7-2005 (JUR 2005\258245), las SSTS de 8-7-2002 (RJ 2002\8939) y 26-9-2002 (RJ 2002\9349), y la SAN de 10-3-2001 (JUR 2001\170088).

[140] Así, en un supuesto de modificación del número y la fecha de caducidad de la tarjeta, la STS de 3-12-1991 (RJ 1991\8955), FJ 5°.

[141] De esta forma, la alteración de la banda magnética supone la generación de una tarjeta *ex novo* e integra por sí misma el delito de falsificación de moneda, independiente del uso posterior fraudulento a que ese instrumento de pago mendaz pueda ser destinado, produciéndose en tal caso una relación concursal entre ambos ilícitos (SSTS de 8-7-2002, RJ 2002\8939, y 26-9-2002, RJ 2002\9349; SSAN de

La introducción en el país y la exportación de moneda falsa o tarjetas falsificadas sólo se sancionan si la realiza persona distinta del falsificador, pues tratándose del mismo sujeto se trata de conductas posteriores ya copenadas con la fabricación.

El transporte también se sanciona de forma independiente sólo en caso de que quien lo realice no haya previamente falsificado, alterado, introducido o exportado el objeto que transporta, pero actúe en connivencia con quien sí lo ha hecho.

La expendición o distribución suponen la puesta en circulación de la moneda o de las tarjetas, por precio en el primer caso, y sin precio en el segundo, en connivencia con el falsificador, alterador, introductor o exportador. En la doctrina se pone en duda que sea aplicable a las tarjetas, pues, se dice, a diferencia de la moneda, que tiene vocación natural de ser expendida o distribuida, las tarjetas no se distribuyen, sino que se utilizan, de forma que no cabría castigar por estas modalidades de acción, así como tampoco por la del párrafo tercero, expendición de tarjetas falsas recibidas de buena fe[142]. Sin embargo, en mi opinión no cabe duda de que las tarjetas falsas pueden distribuirse entre los miembros del grupo organizado para la comisión de futuras estafas, en el sentido que se da a este verbo en la primera acepción del Diccionario de la Real Academia, esto es, «dividir algo entre varias personas, designando lo que a cada una corresponde, según voluntad, conveniencia, regla o derecho»[143].

La tenencia de las tarjetas falsificadas para su expendición o distribución, así como la adquisición de la tarjeta, sabiéndola falsa, para ponerla en circulación, se castigan con la pena inferior en uno o dos grados, «atendiendo al valor de aquélla y al grado de connivencia con los autores mencionados en los números anteriores» (art. 386, segundo párrafo CP), por tanto, con el falsificador, alterador, introductor, exportador, transportista, expendedor o distribuidor. Estas conductas delictivas no son aplicables a quien tiene

30-12-2000, JUR 2001\168588, y 17-7-2006, ARP 2006\713). Entiende que este supuesto «en manera alguna puede entrar en el concepto de "fabricación"», QUINTERO OLIVARES, G., «Fraudes», cit., p. 95. Por el contrario, considera que se respeta el principio de legalidad JAÉN VALLEJO, M., «Falsificación de tarjetas de crédito o débito: la alteración de los datos contenidos en la banda magnética constituye falsificación de moneda (Art. 386 CP)», *RECPC* 04-j10 2002, http://criminet.ugr.es/recpc/jp04/recpc 04-j10.pdf [Fecha de consulta: 9/10/09], pp. 1-3.

[142] Cfr. VILLACAMPA ESTIARTE, C., «La falsificación», cit., pp. 4-5, quien pone de manifiesto además la existencia de otras omisiones en el precepto proyectado.

[143] Cfr. FERNÁNDEZ GARCÍA, E. M., «Los fraudes», cit., p. 122.

en su poder las tarjetas que él mismo ha falsificado, alterado o introducido, ni siquiera a quien las está expendiendo o distribuyendo, sino a quien se prepara para expender o distribuir, siendo sorprendido antes de hacerlo. Estamos ante un delito mutilado de dos actos.

> Por tanto, la mera tenencia de tarjetas falsificadas por un tercero, preordenada a la comisión de un delito contra el patrimonio, por ej., una estafa, no es más que un acto preparatorio impune de éste, sin que pueda castigarse como una modalidad de falsificación de moneda[144].

La adquisición de tarjetas falsas con el fin de ponerlas en circulación se castiga con la misma pena que la tenencia para su expendición o distribución (art. 386, segundo párrafo, último inciso CP). Estamos de nuevo ante un delito mutilado de dos actos.

La expendición o distribución de tarjetas falsas que han sido recibidas de buena fe, después de constarle al sujeto su falsedad, se castiga con la pena de prisión de tres a seis meses o multa de seis a veinticuatro meses, «si el valor aparente de la moneda fuera superior a 400 euros» (art. 386, tercer párrafo CP)[145]. Esta conducta puede parecer difícil de imaginar en relación a las tarjetas, pues si se limita el significado de «expender» a usar o utilizar, la doctrina y la jurisprudencia coinciden en que la utilización de las tarjetas falsas sin haberlas falsificado se lleva a las estafas, y no se considera falsificación de moneda, con lo que este precepto quedaría vacío de contenido en relación a las tarjetas. Frente a ello, hay que puntualizar que «expender» no es sólo gastar o hacer expensas, sino también vender al menudeo, y es perfectamente imaginable el caso de un comerciante que recibe una partida de tarjetas falsificadas y decide venderlas, una vez que le consta su falsedad.

La jurisprudencia admite el delito continuado cuando la falsificación tiene por objeto varias tarjetas en momentos distintos, pero aprovechando idéntica ocasión[146].

---

[144] En la doctrina también hay quien señala que la conducta de distribuir «abarca, además, la de dividir la mercancía entre individuos que se ocuparán del menudeo». ORTS BERENGUER en VIVES ANTÓN, T. S. (coord.), *Comentarios, II*, cit., p. 1729.

[145] Así, la STS de 12-9-2007 (RJ 2007\5081), que corrige la postura contraria mantenida por la SAP de Tarragona de 29-11-2006 (JUR 2007\144141).

[146] Si el valor aparente fuera inferior a 400 euros es aplicable la falta del art. 629 CP, la cual, sin embargo, no hace alusión alguna al concepto extensivo de moneda, planteando la duda de si es aplicable a la falsificación de tarjetas o no. A favor de su aplicación, QUERALT JIMÉNEZ, J. J., *Parte especial*, 5.ª ed. cit., pp. 676-677.

Puesto que la falsificación de tarjetas se equipara por el legislador a la falsificación de moneda, es competente para su enjuiciamiento la Audiencia Nacional, de acuerdo con lo dispuesto en el art. 65.1.b) LOPJ, según el cual «la sala de lo penal de la Audiencia Nacional conocerá: 1. Del enjuiciamiento, salvo que corresponda en primera instancia a los Juzgados Centrales de lo Penal, de las causas por los siguientes delitos: ... b) Falsificación de moneda, delitos monetarios y relativos al control de cambios...». Además, el último inciso del apartado primero del art. 65 LOPJ dispone que «en todo caso, la sala de lo penal de la Audiencia Nacional extenderá su competencia al conocimiento de los delitos conexos con todos los anteriormente reseñados», lo que supone que, aplicando este precepto, deben ser enjuiciados por la Audiencia Nacional los delitos de estafa, estafa informática y falsedad documental relacionados con la falsificación de tarjetas.

La atribución de la competencia de la Audiencia Nacional en relación a la falsificación de tarjetas es pacífica desde el Auto del Tribunal Supremo de 24-1-2003 (RJ 2003\1135)[147], pues con anterioridad, tanto en la jurisprudencia[148], como en la doctrina[149], se afirmaba que la asimilación entre el dinero y la tarjeta prevista en el art. 387 CP sólo pretendía cubrir una laguna de punibilidad, sin que tuviera efectos en orden a determinar la competencia de un tribunal u otro, pues las razones que justifican en ciertos delitos la competencia de la Audiencia Nacional no existirían en el caso de falsificación de tarjetas.

Esta posición tenía su origen en el ya citado Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo, que, en su Acuerdo de

[147] Así, la SAN de 30-12-2000 (JUR 2001\168588).

[148] Seguido por los AATS de 6-3-2003 (JUR 2003\87960), 7-7-2003 (JUR 2003\173479), 16-7-2003 (JUR 2003\202234), 23-7-2003 (JUR 2003\202501), 17-11-2003 (JUR 2003\266606), 24-11-2003 (JUR 2003\273286), 10-12-2003 (JUR 2004\21901), y 22-12-2003 (JUR 2004\22123), entre otros.

[149] ATS de 23-11-1998 (RJ 1998\8977), que afirma que «la equiparación a efectos penales de orden sustantivo no debe extenderse a la materia procesal relativa a la fijación de la competencia, pues las reglas que determinan los asuntos de los que ha de conocer la Sala de lo Penal de la Audiencia Nacional y los Juzgados Centrales de instrucción son una excepción a las normas generales que al respecto ordenan la competencia de los demás órganos judiciales, y que como tales han de ser objeto de interpretación restrictiva». Tan restrictiva, cabe añadir, que es correctora de la clara y diáfana decisión del legislador al respecto, «*contra legem*» e inaceptable. En este sentido, entre otros, FERNÁNDEZ GARCÍA, E. M./LÓPEZ MORENO, J., «La utilización indebida», cit., p. 85.

Esta tesis jurisprudencial se reiteró en los AATS de 7-12-2000 (RJ 2001\6659), en relación a tarjetas prepago de telefónica, y 21-3-2001 (RJ 2001\3551), en relación a tarjetas de crédito.

28 de junio de 2002 (JUR 2002\192448), estimó que «las tarjetas de crédito o débito son medios de pago que tienen la consideración de «dinero de plástico», que el art. 387 del Código Penal equipara a la moneda, por lo que la incorporación a la «banda magnética» de uno de estos instrumentos de pago de unos datos obtenidos fraudulentamente constituye un proceso de falsificación o elaboración que debe ser incardinado en el art. 386 del Código Penal», sin pronunciarse sobre la competencia. En sus primeras resoluciones competenciales, anteriores al referido Pleno, la Sala Segunda del Tribunal Supremo estableció una distinción entre los efectos materiales y los competenciales, estimando por ello que la competencia de la Audiencia Nacional no se extendía a la falsificación de tarjetas de crédito, pese a la equiparación que a efectos punitivos establecía el art. 387 del Código penal de 1995[150]. Sin embargo, este consolidado criterio se modificó en el Auto del Tribunal Supremo de 24-1-2003 (RJ 2003\1135), por estimar que el Acuerdo plenario anteriormente citado, aun cuando no se había pronunciado sobre la competencia, debía determinar, por coherencia, la unificación del enjuiciamiento de todos los comportamientos sancionados a través del art. 387, y se ha mantenido hasta hoy[151].

Lo cierto es que, si bien está justificada para la moneda, no parece tener mucho sentido que la Audiencia Nacional tenga competencia sobre la falsificación de tarjetas[152]. Por lo demás, téngase en cuenta que si la tenencia de tarjetas falsas tiene por objeto su utilización en el comercio, la competencia se determina de acuerdo con las reglas generales, mientras que si tiene por objeto su expendición o distribución, sabiéndola falsa, es competente la Audiencia Nacional[153].

El Proyecto de ley de modificación del Código penal, de 27 de noviembre de 2009, trata de racionalizar la atribución de competencias a la Audiencia Nacional, limitándola a los casos en que la falsificación se realizara en el seno de organizaciones o grupos criminales[154]. En su disposición final primera señalaba que «se modifica el apartado b) del

---

[150] Cfr., entre otros, FERNÁNDEZ ENTRALGO, J., «Falsificación», cit., pp. 37-39.

[151] Vid. los AATS de 23-11-1998 (RJ 1998\8977) y 21-3-2001 (RJ 2001\3551).

[152] AATS de 12-2-2003 (JUR 2003\163440), 7-7-2003 (JUR 2003\173479), 16-7-2003 (JUR 2003\249740), 13-10-2003 (JUR 2003\226968), 18-11-2003 (JUR 2003\262414), 10-12-2003 (JUR 2004\21901), 28-1-2004 (JUR 2004\39100), 29-1-2004 (JUR 2004\39107), 28-2-2004 (JUR 2004\63662), 1-3-2004 (JUR 2004\86089), 18-3-2004 (JUR 2004\114339), 29-4-2004 (JUR 2004\166472), 27-5-2004 (JUR 2004\175373), 18-11-2005 (JUR 2006\47742)...

[153] Cfr. FERNÁNDEZ GARCÍA, E. M., «Los fraudes», cit., p. 123; FERNÁNDEZ GARCÍA, E. M./LÓPEZ MORENO, J., «La utilización indebida», cit., p. 165; QUERALT JIMÉNEZ, J. J., *Parte especial*, 5.ª ed. cit., p. 671.

[154] AATS de 18-2-2004 (JUR 2004\86009), 10-3-2004 (JUR 2004\98517), 1-4-2004 (JUR 2004\114593), 7-12-2004 (JUR 2005\121495), entre otros. En la doctrina, cfr. VILLACAMPA ESTIARTE, C., «La falsificación», cit., p. 3.

artículo 65 de la Ley Orgánica 6/1985 de 1 de julio, del Poder Judicial, que tendrá la siguiente redacción: "b) Falsificación de moneda y fabricación de tarjetas de crédito y débito falsas y cheques de viajero falsos, siempre que sean cometidos por organizaciones o grupos criminales"».

V. Conclusiones

Resulta llamativo que no exista una regulación específica de la suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico en el Código penal. Esta ausencia provoca una serie de consecuencias indeseables: desde la falta de datos oficiales fiables sobre el fenómeno[155], que permite la manipulación interesada de algunos estudios no precisamente imparciales, elaborados por fundaciones o instituciones creadas con el apoyo de empresas que ofrecen productos de seguridad informática, hasta la inseguridad jurídica que provoca la diversidad de tratamientos que a una misma conducta dan los jueces y tribunales, creando desconcierto en los aplicadores del Derecho y desigualdad entre los condenados por hechos similares, si es que no idénticos.

En relación al primer aspecto apuntado, la falta de datos oficiales y la proliferación de estudios con un tono tremendista dan lugar a un discurso informativo impregnado de «*moral panic*» que se ha considerado ejemplo de «*soft surveillance*», en el cual los ciudadanos son animados o incluso requeridos a hacerse responsables de su propia protección[156]. El concepto de «*moral panic*» se ha entendido en la literatura tras la publicación en 1972 de la obra *Folk Devils and Moral Panics*, de Stanley Cohen, en la que se analizaba la alarma social creada a partir de ciertos incidentes entre grupos juveniles. En Estados Unidos no es infrecuente la afirmación de que la suplantación de identidad también se ha convertido en un «*moral panic*»[157]. Y es que, en efecto, numerosos ciudadanos sienten un elevado grado de temor e inseguridad asociado al uso de las tecnologías de la información y

[155] A favor de esta modificación, VILLACAMPA ESTIARTE, C., «La falsificación», cit., p. 4.

[156] Ni las estadísticas judiciales ni las del Ministerio del Interior pueden ofrecer datos válidos sobre la prevalencia de esta forma de criminalidad. Los únicos datos con que se puede contar son los estudios realizados por diversas entidades, oficiales o privadas, fundamentalmente vinculadas a la promoción de los servicios de la sociedad de la información, en particular el comercio electrónico. Normalmente los datos que ofrecen se basan en encuestas a diversos sectores de la población.

[157] Cfr. COLE, S. A./PONTELL, H. N., «Don't Be Low Hanging Fruit: Identity Theft as Moral Panic», en MONAHAN, T. (Ed.), *Surveillance and Security. Technological Politics and Power in Everyday Life*, Routledge, New York-London, 2006, p. 126.

las comunicaciones en el comercio, sobre todo electrónico, sin haber sufrido personalmente ningún incidente de suplantación de identidad, pero habiendo recibido numerosa información en los medios de comunicación y por otras vías acerca de la extensión y gravedad de este fenómeno criminal[158].

También llama la atención que tanto el Estado como otros agentes corporativos, tradicionalmente concebidos en el discurso de la seguridad como actores orwellianos insaciables en su afán de extender su capacidad de vigilancia e intrusión en la intimidad de los ciudadanos tan lejos como resulte posible, se muestren reticentes a la hora de implementar medidas de seguridad en el comercio que eviten la suplantación de identidad, pues sin duda la mejor forma de poner coto a la utilización fraudulenta de datos de identidad en el comercio tradicional y electrónico es el aumento de la seguridad de la información personal que obra en manos de la Administración y de empresas privadas[159] y la implantación de nuevas medidas tecnológicas que permitan la verificación de la identidad del usuario[160], por ej., basadas en sistemas biométricos[161]. Ahora bien, esta actitud es consistente con la ética neoliberal de las décadas pasadas, que anima a los

---

[158] Por todos, COLE, S. A./PONTELL, H. N., «Don't Be Low Hanging Fruit», cit., pp. 125 ss; MONAHAN, T., «Identity Theft Vulnerability», *Theoretical Criminology*, Vol. 13, N.º 2, 2009, pp. 156 ss; NESBITT, F., «The real fraud?», en la página web http://www.ikmagazine.com/xq/asp/txtSearch.search+retrieval/exactphrase.0/sid.0/articleid.FB131054-4BAD-4BCD-957D-22996D039479/qx/display.htm. Trata extensamente la cuestión MCNALLY, M. M., *Trial by circumstance: is identity theft a modern-day moral panic?*, Newark, 2008, *passim*.

[159] En Estados Unidos lo resalta POSTER, M., *Information Please: Culture and Politics in the Age of Digital Machines*, Duke University Press, Durham, 2006, p. 94.

[160] Es una observación generalizada en la doctrina. Vid. por todos COLLINS, J. M./HOFFMAN, S. K., *Identity theft victims' assistance guide: The process of healing*, Looseleaf Law, New York, 2004, p. 6; MONAHAN, T., «Identity Theft Vulnerability», cit., pp. 166 ss; STANA, R. M., «Identity Theft: Prevalence and Cost Appear to be Growing», en HAYWARD, C. L. (Ed.), *Identity Theft*, Novinka Books, New York, 2004, pp. 27-28; WHITSON, J. R./HAGGERTY, K. D., «Identity theft and the care of the virtual self», *Economy and Society* Vol. 37, N.º 4, 2008, p. 589.

[161] Cfr. FLETCHER, N., «Challenges for regulating financial fraud in cyberspace», *Journal of financial fraud* Vol. 14, N.º 2, 2007, p. 193; GRABOSKY, P./SMITH, R./DEMPSEY, G., *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press, Cambridge, 2001, p. 128. Esa verificación es interesante no sólo para evitar la suplantación de identidad, sino también respecto a la protección de menores, al permitir evitar que tengan acceso a contenidos potencialmente dañinos para ellos. Sobre las técnicas empleadas para controlar la edad, vid. SIEBERT, J., «Protecting Minors on the Internet: An Example from Germany», en MÖLLER, C./AMOUROUX, A. (Ed.), *Governing the Internet Freedom and Regulation in the OSCE Region*, disponible en la página web http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf [Fecha de consulta: 9/10/09], pp. 147 ss.

ciudadanos a protegerse a sí mismos porque el Estado no quiere o no puede hacerlo[162], responsabilizando al mismo tiempo a quienes no se protegen suficientemente[163], sin tener en cuenta que buena parte de las medidas aconsejadas no están precisamente al alcance de todos, dado el bajo nivel de conocimientos informáticos de la población en general[164]. Esta actitud permite desviar a las víctimas la responsabilidad por los costes económicos y sociales de los riesgos producidos[165].

En relación al segundo aspecto apuntado, en este trabajo se ha puesto de manifiesto la existencia de opiniones doctrinales y resoluciones jurisprudenciales contradictorias en relación a supuestos de hecho similares, si es que no idénticos. Ello no redunda precisamente en beneficio de la seguridad jurídica. Sería deseable una clarificación a través de una reforma futura del Código penal que tenga en cuenta las críticas vertidas en torno a la regulación actual.

VI. Bibliografía

ALONSO CONDE, A. B., *Comercio electrónico: antecedentes, fundamentos y estado actual*, Universidad Rey Juan Carlos/Dykinson, Madrid, 2004.
ANTÓN ONECA, J., *Las estafas y otros engaños*, Seix, Barcelona, 1957.

[162] Sobre las ventajas y desventajas de estos sistemas, NEWTON, E. M., «Strengths and Weaknesses of Biometrics», en CAMP, L. J., *Economics of Identity Theft. Avoidance, Causes and Possible Cures*, Springer, New York, 2007, pp. 109 ss. Ha de tenerse en cuenta que algunos identificadores biométricos cambian con el transcurso del tiempo, como ocurre con la voz, lo que supone un alto índice de errores. Por el contrario, algunos autores ponen de relieve el problema que podría suponer que un identificador biométrico esté comprometido, como puede ocurrir con la huella dactilar, al ser imposible cambiarla. Así, MAY, D. A./HEADLEY, J. E., *Identity theft*, Peter Lang, New York, 2004, p. 63.

[163] Cfr. MARX, G. T., «Soft Surveillance»: The Growth of Mandatory Volunteerism in Collecting Personal Information – «Hey Buddy Can You Spare a DNA?», en MONAHAN, T. (Ed.), *Surveillance and Security. Technological Politics and Power in Everyday Life*, Routledge, New York-London, 2006, p. 49; MONAHAN, T., «Identity Theft Vulnerability», cit., pp. 155 ss, quien destaca el provecho que saca la industria de todo ello (p. 156).

[164] Lo que MARX, G. T., «Soft Surveillance», cit., p. 52, denomina «blame-the-victim *caveat subjectus* logic». Vid. también MCNALLY, M. M., *Trial by circumstance*, cit., p. 326; WHITSON, J. R./HAGGERTY, K. D., «Identity theft», cit., pp. 572-594. Insiste en esta dirección MONAHAN, T., «Identity Theft Vulnerability», cit., pp. 159 ss, destacando la relación entre la autoprotección y el consumo de productos de seguridad.

[165] Como ponen de manifiesto WHITSON, J. R./HAGGERTY, K. D., «Identity theft», cit., p. 588.

[166] WHITSON, J. R./HAGGERTY, K. D., «Identity theft», cit., p. 591.

ARÁNGUEZ SÁNCHEZ, C., *La falsificación de moneda*, Bosch, Barcelona, 2000.
BACIGALUPO ZAPATER, E., «Utilización abusiva de cajeros automáticos por terceros no autorizados», *Poder Judicial* núm. especial IX, 1988, pp. 85-95.
BAJO FERNÁNDEZ, M. (Dir.), *Compendio de Derecho Penal (Parte Especial)*, II, Ceura, Madrid, 1998.
BAJO FERNÁNDEZ, M./DÍAZ-MAROTO y VILLAREJO, J., *Manual de Derecho penal. Parte especial, III*, 3.ª ed. Ceura, Madrid, 1995.
BAJO FERNÁNDEZ, M., «Artículo 248», en COBO DEL ROSAL, M. (Dir.), *Comentarios al Código penal. Tomo VIII. Delitos contra el patrimonio y contra el orden socioeconómico. Artículos 234 a 272*, EDERSA, Madrid, 2005, pp. 235-299.
BATUECAS CALETRIO, A., *Pago con tarjeta de crédito. Naturaleza y régimen jurídico*, Thomson-Aranzadi, Cizur Menor, 2005.
BERG, T., «The Changing Face of Cybercrime – New Internet Threats create Challenges to Law Enforcement Agencies», *Michigan Bar Journal* June 2007, pp. 18-22, disponible en la página web http://www.michbar.org/journal/pdf/pdf4article1163.pdf [Fecha de consulta: 9/10/09].
BOIX REIG, J., *El delito de usurpación de estado civil*, Universidad de Valencia, Valencia, 1980.
BOIX REIG, J./JAREÑO LEAL, A., «De la usurpación del estado civil», en VIVES ANTÓN, T. S. (Coord.), *Comentarios al Código Penal de 1995. Volumen II (Art. 234 a Disposiciones Finales)*, Tirant lo Blanch, Valencia, 1997, pp. 1763 ss.
BOLEA BARDÓN, C./ROBLES PLANAS, R., «La utilización de tarjetas ajenas en cajeros automáticos: ¿Robo, hurto o estafa?», *La Ley* 2001-4, pp. 1447-1453.
CALLE RODRÍGUEZ, M. V., «El delito de estafa informática», *La Ley Penal* núm. 37, abril 2007, pp. 40-56.
CAMP, L. J., *Economics of Identity Theft. Avoidance, Causes and Possible Cures*, Springer, New York, 2007.
CASTILLA CUBILLAS, M., *La tarjeta de crédito*, Marcial Pons, Madrid-Barcelona, 2007.
CHAWKI, M./ABDEL WAHAB, M. S., «Identity Theft in Cyberspace: Issues and Solutions», *Lex Electronica* Vol. 11, Nr. 1, 2006, disponible en la página web www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf [Fecha de consulta: 9/10/09], pp. 1-41.
CHOCLÁN MONTALVO, J. A., «Estafa por computación y criminalidad económica vinculada a la informática», *AP* 1997-2, margs.1069-1094.
—, «Fraude informático y estafa por computación», en LÓPEZ ORTEGA, J. J. (Dir.), *Internet y Derecho penal*, CDJ X-2001, CGPJ, Madrid, 2001, pp. 305-352.
—, «Infracciones patrimoniales en los procesos de transferencia de datos», en MORALES GARCÍA, O. (Dir.), *Delincuencia informática. Problemas de responsabilidad*, Cuadernos de Derecho Judicial IX-2002, CGPJ, Madrid, 2002, pp. 241-280.
COLE, S. A./PONTELL, H. N., «Don't Be Low Hanging Fruit»: Identity Theft as Moral Panic», en MONAHAN, T. (Ed.), *Surveillance and Security. Technological Politics and Power in Everyday Life*, Routledge, New York-London, 2006, pp. 125-147.

COLLINS, J., *Preventing Identity Theft Into Your Business*, John Wiley, New Jersey, 2005.

COLLINS, J. M./HOFFMAN, S. K., *Identity theft victims' assistance guide: The process of healing*, Looseleaf, New York, 2004.

CONDE-PUMPIDO FERREIRO, C., *Estafas*, Tirant lo Blanch, Valencia, 1997.

CÓRDOBA RODA, J./GARCÍA ARÁN, M. (Dirs.), *Comentarios al Código penal. Parte especial. Tomo I*, Marcial Pons, Madrid-Barcelona, 2004.

CÓRDOBA RODA, J., «Artículo 401», en CÓRDOBA RODA, J./GARCÍA ARÁN, M. (Dirs.), *Comentarios al Código Penal. Parte Especial. Tomo II*, Marcial Pons, Madrid-Barcelona, 2004, pp. 1877-1879.

CREMADES GARCÍA, J., «El fraude en los servicios financieros "on-line"», en AA.VV., *Estudios jurídicos. Ministerio Fiscal. II-2003. Delincuencia Informática. Drogas de abuso: Aspectos Científicos y Jurídicos. Experiencias aplicativas de la LORPM*, Ministerio de Justicia, Madrid, 2004, pp. 249-284.

CUELLO CALÓN, E., *Derecho penal. Tomo II (Parte especial)*, 14.ª ed. Bosch, Barcelona, 1975.

FARALDO CABANA, P., «Los conceptos de manipulación informática o artificio semejante en el delito de estafa informática», *Eguzkilore. Cuadernos del Instituto Vasco de Criminología* 2007, núm. 21, pp. 33-57.

—. *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Tirant lo Blanch, Valencia, 2009.

FEDERAL TRADE COMMISSION, *Consumer Fraud and Identity Theft Complaint Data January-December 2005*, 2006, pp. 1-70, disponible en la página web www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf [Fecha de consulta: 9/10/09].

FERNÁNDEZ ENTRALGO, J., «Falsificación y utilización fraudulenta de tarjetas electrónicas», en MAZA MARTÍN, J. M. (Dir.), *Tarjetas bancarias y Derecho penal*, CDJ VI-2002, CGPJ, Madrid, 2003, pp. 13-66.

FERNÁNDEZ GARCÍA, E. M., «Fraudes y otros delitos patrimoniales relacionados con la informática e Internet», en AA.VV., *Estudios jurídicos. Ministerio Fiscal. IV-1999*. Ministerio de Justicia, Madrid, 1999.

—, «Los fraudes con tarjetas de pago y otros supuestos de delincuencia informática patrimonial. Incidencia de la Reforma Penal», en AA.VV., *Estudios jurídicos. Ministerio Fiscal. II-2003. Delincuencia Informática. Drogas de abuso: Aspectos Científicos y Jurídicos. Experiencias aplicativas de la LORPM*, Ministerio de Justicia, Madrid, 2004, pp. 105-208.

FERNÁNDEZ GARCÍA, E. M./LÓPEZ MORENO, J., «La utilización indebida de tarjetas de crédito en el Código Penal de 1995», *Revista del Poder Judicial* núm. 46, 1997, pp. 143-216.

FERNÁNDEZ TERUELO, J. G., *Cibercrimen. Los delitos cometidos a través de Internet*, CCC, s/l, 2007.

—, «Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de la red», *RDPC* núm.19, enero 2007, pp. 217-243.

FLETCHER, N., «Financial fraud in cyberspace», *Journal of financial fraud* Vol. 14, N.º 2, 2007, pp. 190-207.

FRAMIÑÁN SANTAS, J., «Medios de pago *on line* a través de Internet», en GÓMEZ SEGADE, J. A. (Dir.), *Comercio electrónico en Internet*, Marcial Pons, Madrid-Barcelona, 2001, pp. 373-396.

FUENTE HONRUBIA, F. de la, «La usurpación de estado civil», *Actualidad Penal* 2000-1, margs.145-157.

GALÁN MUÑOZ, A., *El fraude y la estafa mediante sistemas informáticos. Análisis del art. 248.2 CP*, Tirant lo Blanch, Valencia, 2005.

GALLEGO SOLER, J. I., «Fundamento y límites de los deberes de autoprotección de la víctima en la estafa», *ADPCP* Tomo LVIII, Fasc. II, mayo-agosto 2005, pp. 529-559.

GERCKE, M., *Internet-related Identity Theft*, informe para el Consejo de Europa, 2007, p. 7, disponible en la página web http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/Internet_related_identity_theft_%20Marco_Gercke.pdf [Fecha de consulta: 9/10/09].

GONZÁLEZ RUS, J. J., «Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», *Poder Judicial* núm. especial IX, 1988, pp. 39-52.

—, «Protección penal de sistemas, elementos, datos, documentos y programas informáticos», *RECPC* 01-14 (1999), http://criminet.ugr.es/recpc/recpc_01-14.html [Fecha de consulta: 19/10/09].

GORDILLO ÁLVAREZ-VALDÉS, I., «Falsedades», en LAMARCA PÉREZ, C. (Coord.), *Derecho Penal. Parte especial*, 4.ª ed. Colex, Madrid, 2008, pp. 563-593.

GRABOSKY, P./SMITH, R./DEMPSEY, G., *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press, Cambridge, 2001.

GUTIÉRREZ FRANCÉS, M. L., *Fraude informático y estafa*, Ministerio de Justicia, Madrid, 1991.

—, «Delincuencia económica e informática en el nuevo Código Penal», en GALLARDO ORTIZ, M. A. (Dir.), *Ámbito jurídico de las tecnologías de la información*, CGPJ, Madrid, CDJ XI-1996, pp. 247-305.

HANSEN, M./MEISSNER, S. (Hrsg.), *Verkettung digitaler Identitäten*, disponible en la página web https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf, [Fecha de consulta: 9/10/09].

HAYWARD, C. L. (Ed.), *Identity Theft*, Novinka Books, New York, 2004.

HERRERA MORENO, M., «El fraude informático en el derecho penal español», *Actualidad Penal* 2001-3, margs. 925-964.

HOAR, S. B., «Identity Theft», *Oregon Law Review* 80, 2001, 1423.

—, «Trends in Cybercrime», *Criminal Justice* 20, 3, 2005, pp. 4-13.???

JAÉN VALLEJO, M., «Falsificación de tarjetas de crédito o débito: la alteración de los datos contenidos en la banda magnética constituye falsificación de moneda (Art. 386 CP). Nota sobre el Acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo de 28 de junio de 2002», *RECPC* 04-j10 2002, pp. 1-3, http://criminet.ugr.es/recpc/jp04/recpc04-j10.pdf [Fecha de consulta: 19/10/09].

JAVATO MARTÍN, A. M., «Análisis de la jurisprudencia penal en materia de medios electrónicos de pago», en MATA Y MARTÍN, R. M. (Dir.), *Los medios electrónicos de pago. Problemas jurídicos*, Comares, Granada, 2007, pp. 367-382.

LASCURAIN SÁNCHEZ, J. A., «De las falsedades», en RODRÍGUEZ MOURULLO, G. (Dir.), *Comentarios al Código Penal*, Civitas, Madrid, 1997, pp. 1054 ss.

LÓPEZ BARJA DE QUIROGA, J., «El moderno derecho penal para una sociedad de riesgos», *Revista del Poder Judicial* núm.48, 1997, pp. 289-321.

MANES, V., «La incidencia de las «decisiones marco» en la interpretación en materia penal: perfiles de derecho sustantivo», *RECPC* (en línea) núm. 09-07, disponible en la página web http://criminet.ugr.es/recpc/09/recpc09.html [Fecha de consulta: 19/10/09], pp. 1-20.

MARTÍNEZ GONZÁLEZ, M., «Mecanismos de seguridad en el pago electrónico», en MARX, G. T., «Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information – «Hey Buddy Can You Spare a DNA?», en MONAHAN, T. (Ed.), *Surveillance and Security. Technological Politics and Power in Everyday Life*, Routledge, New York-London, 2006, pp. 37-56.

MATA BARRANCO, N. de la, «Utilización abusiva de cajeros automáticos: apropiación de dinero mediante la tarjeta sustraída a su titular», *Poder Judicial* núm. especial IX, 1988, pp. 151-174.

MATA Y MARTÍN, R. M. (Dir.), *Los medios electrónicos de pago. Problemas jurídicos*, Comares, Granada, 2007, pp. 5-66.

MATA Y MARTÍN, R. M., *El delito de robo con fuerza en las cosas*, Tirant lo Blanch, Valencia, 1995.

—, *Delincuencia informática y Derecho penal*, Edisofer, Madrid, 2001.

—, «Criminalidad Informática: una introducción al cibercrimen», en RUIZ MIGUEL, C., y otros, *Temas de Direito da Informática e da Internet*, Coimbra Editora, Coimbra, 2004, pp. 197-236.

—, *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*, Thomson-Aranzadi, Cizur Menor, 2007.

—, «Medios electrónicos de pago y delitos de estafa», en MATA Y MARTÍN, R. M. (Dir.), *Los medios electrónicos de pago. Problemas jurídicos*, Comares, Granada, 2007, pp. 319-365.

MATELLANES RODRÍGUEZ, N., «Algunas notas sobre las formas de delincuencia informática en el Derecho penal», en DIEGO DÍAZ-SANTOS, R./SÁNCHEZ LÓPEZ, V. (Coords.), *Hacia un Derecho penal sin fronteras*, Colex, Madrid, 2000, pp. 129-147.

MAY, D. A./HEADLEY, J. E., *Identity Theft*, Peter Lang, New York, 2004.

MCNALLY, M. M., *Trial by circumstance: is identity theft a modern-day moral panic?*, Newark, 2008.

MONAHAN, T., «Identity Theft Vulnerability», *Theoretical Criminology* Vol. 13, N.º 2, 2009, pp. 155-176.

MORILLAS CUEVA, L., «Falsedades (III). Falsedades personales», en COBO DEL ROSAL, M. (Coord.), *Derecho Penal Español. Parte Especial*, 2.ª ed., Dykinson, Madrid, 2005, pp. 849 ss.

—, «Artículo 255», en COBO DEL ROSAL, M. (Dir.), *Comentarios al Código penal. Tomo VIII. Delitos contra el patrimonio y contra el orden socioeconómico. Artículos 234 a 272*, EDERSA, Madrid, 2005, pp. 511-549.

MUÑOZ CONDE, F., *Derecho Penal. Parte Especial*, 16.ª ed. Tirant lo Blanch, Valencia, 2007.

MUÑOZ DE MORALES ROMERO, M., «La aplicación del principio de interpretación conforme a las decisiones-marco: ¿hacia el efecto directo?: especial

referencia al caso *Pupino*», en ARROYO ZAPATERO, L./NIETO MARTÍN, A. (Dirs.), *El Derecho penal de la Unión Europea. Situación actual y perspectivas de futuro*, Ediciones de la Universidad de Castilla-La Mancha, Cuenca, 2007, pp. 291-323.

NEWTON, E. M., «Strengths and Weaknesses of Biometrics», en CAMP, L. J., *Economics of Identity Theft. Avoidance, Causes and Possible Cures*, Springer, New York, 2007, pp. 109-124.

ORTS BERENGUER, E./ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia, 2001.

PACHECO, J. F., *El Código Penal. Concordado y comentado*, Edisofer, Madrid, 2000 (reedición de la 3.ª de 1867).

PÉREZ PELLICER, A., «La estafa de crédito», en BOIX REIG, J. (Dir.), *Estafas y falsedades (Análisis jurisprudencial)*, Iustel, Madrid, 2005, pp. 112-158.

POSTER, M., *Information Please: Culture and Politics in the Age of Digital Machines*, Duke University Press, Durham, 2006.

QUERALT JIMÉNEZ, J. J., *Derecho Penal Español. Parte especial*, 5.ª ed. Atelier, Barcelona, 2008.

QUINTERO OLIVARES, G. (Dir.), *Comentarios a la Parte Especial del Derecho Penal*, 7.ª ed. Thomson-Aranzadi, Cizur Menor, 2008.

QUINTERO OLIVARES, G., «Fraudes y defraudaciones ante una reforma del Código penal», en ARROYO ZAPATERO, L., y otros, *La reforma del Código penal tras 10 años de vigencia*, Thomson-Aranzadi, Cizur Menor, 2006, pp. 81-102.

—, «Artículo 401», en QUINTERO OLIVARES G. (Dir.), *Comentarios al Código Penal. Tomo III. Parte Especial (Artículos 319 a DF 7.ª)*, 5.ª ed., Thomson-Aranzadi, Cizur Menor, 2008, pp. 509-512.

—, «De la usurpación de funciones públicas y del intrusismo», en QUINTERO OLIVARES, G. (Dir.), *Comentarios al Código Penal. Tomo III. Parte Especial (Artículos 319 a DF 7.ª)*, 5.ª ed., Thomson-Aranzadi, Cizur Menor, 2008, pp. 513-522.

RODRÍGUEZ DEVESA, J. M., *Derecho penal español. Parte especial*, 6.ª ed. Madrid, 1975.

RODRÍGUEZ MOURULLO, G. (Dir.), *Comentarios al Código penal*, Civitas, Madrid, 1997.

RODRÍGUEZ MOURULLO, G./ALONSO GALLO, J./LASCURAÍN SÁNCHEZ, J. A., «Derecho Penal e Internet», en CREMADES, J./FERNÁNDEZ-ORDÓÑEZ, M. A./ILLESCAS, R. (coords.), *Régimen jurídico de Internet*, La Ley, Madrid, 2002, pp. 257-307.

ROMEO CASABONA, C. M., *Poder informático y seguridad jurídica*, Fundesco, Madrid, 1988.

—, «Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos», *Poder Judicial* número especial IX, 1988, pp. 109-130.

ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Comares, Granada, 2002.

RUIZ RODRÍGUEZ, L. R., «Uso ilícito y falsificación de tarjetas bancarias» [artículo en línea]. *IDP. Revista de Internet, Derecho y Política* núm. 3, 2006 [Fecha de consulta: 19/10/09]. http://www.uoc.edu/idp/3/dt/esp/ruiz.pdf>

SIEBERT, J., «Protecting Minors on the Internet: An Example from Germany», en MÖLLER, C./AMOUROUX, A. (Ed.), *Governing the Internet Freedom and Regulation in the OSCE Region*, disponible en la página web http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf [Fecha de consulta: 9/10/09], 2007, pp. 147-162.

SILVA SÁNCHEZ, J. M. (Dir.), *Lecciones de Derecho penal. Parte especial*, 2.ª ed. Atelier, Barcelona, 2009.

STANA, R. M., «Identity Theft: Prevalence and Cost Appear to be Growing», en HAYWARD, C. L. (Ed.), *Identity Theft*, Novinka Books, New York, 2004, pp. 17-72.

STUCKENBERG, C.-F., «Zur Strafbarkeit von "Phising"», *ZStW* 2006, Vol. 118, Heft 4, pp. 878-912.

THORHALLSSON, J., «An User Perspective on Spam and Phishing», en MÖLLER, C./AMOUROUX, A. (Ed.), *Governing the Internet Freedom and Regulation in the OSCE Region*, disponible en la página web http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf [Fecha de consulta: 9/10/09], 2007, pp. 201-220.

VALLE MUÑIZ, J. M., *El delito de estafa. Delimitación jurídico penal con el fraude civil*, Bosch, Barcelona, 1987.

VELASCO NÚÑEZ, E., «Fraudes informáticos en red: del *phising* al *pharming*», *La Ley Penal* núm.37, abril 2007, pp. 57-66.

—, «Estafa informática y banda organizada. *Phishing, pharming, smishing* y "muleros"», *La Ley Penal* núm. 49, mayo 2008, pp. 19-29.

VILLACAMPA ESTIARTE, C., *La falsedad documental: análisis jurídico-penal*, Cedecs, Barcelona, 1999.

—, «La falsificación de medios de pago distintos del efectivo en el Proyecto de Ley Orgánica de Reforma del CP de 2007: ¿respetamos las demandas armonizadoras de la Unión Europea?», *Diario La Ley* núm.6994, 22 de julio de 2008, pp. 1-7.

VIVES ANTÓN, T. S. (Coord.), *Comentarios al Código Penal de 1995. Volumen II (Art. 234 a Disposiciones Finales)*, Tirant lo Blanch, Valencia, 1996.

VIVES ANTÓN, T. S., y otros, *Derecho Penal. Parte Especial*, 2.ª ed. Tirant lo Blanch, Valencia, 2008.

WHITSON, J. R./HAGGERTY, K. D., «Identity theft and the care of the virtual self», *Economy and Society* Vol. 37, N.º 4, 2008, pp. 572-594.