Universidad de Valladolid

Facultad de Derecho

Grado en Derecho

El Fraude Informático y Telemático:

Perspectiva Penal

Presentado por:

Alberto Molinos Cóbreces

Tutelado por:

Antonio María Javato Martín

Valladolid, 22 de junio de 2020

ÍNDICE

RESUMEN

El presente trabajo tiene como finalidad ofrecer una visión global acerca de los tipos penales contenidos en el artículo 248.2 a) y c) de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (en lo siguiente CP), que contienen la estafa informática y telemática, y la estafa llevada a cabo mediante el uso de tarjetas de crédito o débito, cheques de viaje, o los datos contenidos en ellas respectivamente.[1]

A lo largo del trabajo se desarrollarán cuestiones tanto de derecho penal, como de derecho procesal, así como la respuesta dada frente a este delito por la Unión Europea (en adelante UE) y en el ámbito internacional. Tendrán cabida además consideraciones criminológicas acerca de este tipo de delincuencia.

Son objeto de estudio, en primer lugar, estas consideraciones criminológicas, identificando posteriormente las decisiones tomadas frente a este problema a nivel transnacional. Seguidamente, se procederá a analizar el contenido del art. 248 del CP. Tras ello, nos ocuparemos de los problemas concursales para finalmente, ofrecer unas conclusiones que contendrán las oportunas consideraciones de política criminal.

---

[1] Artículo 248

1. 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.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Para el desarrollo de estas cuestiones se hará uso de fuentes normativas, doctrinales y jurisprudenciales que den apoyo a la materia expuesta.

Palabras clave: Estafa. Estafa informática. Fraude informático y telemático. Tarjetas de crédito y débito. Estafa electrónica. Manipulación informática. Engaño. Internet. Derecho Penal.

ABSTRACT

The porpouse of the present work is to offer an overview of the criminal types contained in the article 248.2 a) and c) of the Organic Law 10/1995, of November 23, of the Penal Code (in the following CP), which contain the computer scam and the scam carried out through the use of credit or debit cards, travelers checks, or the data contained therein respectively.

Throughout the work, criminal law issues will be developed, as well as the response given to this crime by the European Union and internationally. There will also be room for criminological considerations regarding this type of crime.

These criminological considerations are the object of study in the first place, subsequently identifying the decisions taken regarding this problem at the transnational level. Afterwards, the content of the article 248 of the Penal Code will be analysed. Then, we will deal with bankruptcy problems, to finally offer some conclusions that will contain the appropriate considerations of criminal policy.

For the development of these issues, use will be made of normative, doctrinal and jurisprudential sources that give support to the exposed matter.

Key words: Criminal fraud. Computer fraud. Credit and debit cards. Phishing. Computer manipulation. Deceit. Internet. Criminal Law.

1. INTRODUCCIÓN

La necesidad de comunicarse y transmitir información inherente al hombre ha llevado al desarrollo de diferentes medios de transmitirla, desde las señales de humo, el código Morse hasta llegar al nacimiento de la informática, que engloba todas aquellas máquinas y métodos que son utilizados para el procesamiento de información y para la ayudar al hombre en el desarrollo de trabajos rutinarios y repetitivos. Como consecuencia de los avances en el mundo de la informática surgió Internet, una tecnología que permite el acceso a la cultura, la ciencia y la información a millones de personas en el mundo.[2]

La rapidez con la que se producen avances tecnológicos en una gran variedad de ámbitos, [3] así como la progresiva ampliación de las relaciones transfronterizas entre Estados ha posibilitado la ampliación de las formas de cometer actos ilícitos a nivel mundial, haciendo uso de las nuevas tecnologías y de la informática. Las nuevas tecnologías han repercutido entre otras esferas en la intimidad, en aquellos supuestos de revelación o difusión de manera ilegal de datos personales. Además, pueden ser utilizadas para la transmisión de contenido ilícito, como pornografía infantil, así como afectar al patrimonio y a orden socioeconómico, aspecto este último que será el objeto primordial de análisis de este trabajo.[4]

Las estrategias seguidas por el legislador a lo largo de este proceso de desarrollo tecnológico han sido entre otras la introducción de figuras penales

---

[2] FERNÁNDEZ ROZAS, JC. Nuevas disposiciones de la Unión Europea sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Disponible en: https://fernandezrozas.com/2019/05/15/nuevas-disposiciones-de-la-union-europea-sobre-la-lucha-contra-el-fraude-y-la-falsificacion-de-medios-de-pago-distintos-del-efectivo/(consulta 23/05/2020).

[3] PALOMINO MARTIN, J.M. Derecho penal y nuevas tecnologías. Hacia un sistema informático para la aplicación del derecho penal. Valencia, pp.33-41.

[4] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, p.24.

paralelas a las tradicionales, en las que se incorpora a cada tipo el equivalente mediante el uso de nuevas tecnologías. Debido a esta confusión, se afirma que no existe un bien jurídico propio en relación a los delitos informáticos, sino que coincide con el protegido en los tipos penales tradicionales, o bien introduce nuevos objetos materiales del delito que se encuentran incorporados al uso de la tecnología. De este modo, se han ido cubriendo poco a poco las lagunas de punibilidad, que han ido poniendo de manifiesto la jurisprudencia según surgían nuevas modalidades de comisión de esta clase delitos.[5]

Dentro de la adaptación legislativa que se ha producido, es ámbito de estudio de este trabajo la modificación del artículo 248 del CP mediante la LO 5/2010 de 22 de junio, que recoge en su número primero la estafa tradicional y en el segundo la estafa informática en la letra a), el uso de programas de ordenador concebidos para llevar a cabo estafas en la letra b) y el uso de tarjetas o sus datos para este fin en la letra c), siendo éste último tipo delictivo el incluido tras la reforma.[6]

2. CRIMINOLOGÍA Y NUEVAS TECNOLOGÍAS

2.1. RELEVANCIA DEL FRAUDE INFORMÁTICO

La relevancia de los delitos informáticos ha sufrido un crecimiento exponencial a lo largo de los años, como consecuencia del incremento del denominado ciberespacio y el consecuente aumento de la ciberpoblación en el ámbito de Internet; hasta el punto de que las compañías de seguros de diversos países vienen ofreciendo cobertura frente a ellos.[7]

---

[5] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, pp..25-27.

[6] SILVA SÁNCHEZ, J.M. El nuevo código penal. Comentarios a la reforma. Madrid, pp. 337 y ss.

[7] RAMÍREZ BEJERANO, EE. Y AGUILERA RODRÍGUEZ, AR. Los delitos informáticos. Tratamiento Internacional, Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm (consulta 20/04/2020).

En EEUU se calcula que los perjuicios económicos generados superan los 10000 millones de dólares, así como más de 5000 millones de libras esterlinas en Reino Unido. Según el FBI, el 90% de los delitos informáticos investigados en Estados Unidos están relacionados con internet, lo que refleja la realidad de la inexistencia de fronteras en el ámbito de las nuevas tecnologías. Para solucionarlo, se debe de establecer una coordinación internacional a la hora de investigar, así como a la de aplicar leyes que cuenten con un núcleo común. [8]

En España, se han registrado en 2019 un total de 218302 ciberdelitos, de los cuales 192375 fueron fraudes informáticos, lo que supone un acusado incremento en comparación con los 37458 ciberdelitos que se registraron en 2011, de los cuales 21075 fueron calificados de fraude informático[9]. Al igual que en otros países, se ha creado un Grupo que se encarga de manera exclusiva de actuar frente a los delitos informáticos. Se trata de la Brigada Central de Investigación Tecnológica(BCIT), unidad policial encargada de obtener pruebas y perseguir delincuentes, para poner unas y otros posteriormente a disposición judicial. Se encuentra encuadrada en la Unidad de Investigación Tecnológica del Consejo General del Poder General, que se trata del órgano de la Dirección General de la Policía encargado de investigar y perseguir el ciberdelito en el ámbito nacional y transnacional.[10]

En el ámbito de la Guardia Civil, la investigación de los delitos informáticos más complejos la lleva a cabo el Grupo de delitos Telemáticos(GDT), que se trata de una unidad más especializada y con ámbito

[8]RAMÍREZ BEJERANO, EE. Y AGUILERA RODRÍGUEZ, AR. Los delitos informáticos. Tratamiento Internacional, Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm (consulta 20/04/2020).

[9] ESTADISTICAS - OEDI | Observatorio Español Delitos Informáticos. Disponible en: https://oedi.es/estadisticas/ (consulta 14/05/2020).

[10]Página oficial de la DGP-Comisaría General de Policía Judicial. Disponible en: https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html (consulta 14/05/2020).

de actuación en todo el territorio nacional. El resto de investigaciones las realizan los Equipos de Investigación Tecnológica(EDITE,s) que se encuentran desplegados por cada una de las provincias de España .[11]

En la lucha contra la ciberdelincuencia cabe mencionar a su vez la labor llevada a cabo por el Instituto Nacional de Ciberseguridad(INCIBE), que se trata de una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Se encarga del desarrollo de la ciberseguridad a nivel nacional e internacional, mediante una labor basada en la investigación, prestación de servicios y coordinación con los agentes competentes en la materia.[12]

2.2. SUJETO ACTIVO DEL FRAUDE INFORMÁTICO

Los delitos informáticos suelen cometerse por aquellas personas que poseen una serie de habilidades o características de las que el común de los delincuentes carece. Estas pasan por el manejo de sistemas informáticos, de modo que los delincuentes generalmente se encuentran en lugares estratégicos para el desarrollo de esta clase de habilidades atendiendo a su situación laboral, aunque en otros casos la actividad laboral no influye en la facilitación de la comisión de esta clase de delitos.

Según un estudio publicado en el manual de las Naciones Unidas sobre la prevención y control de los delitos informáticos (#43 y #44), el 90% de los delitos que se realizaron por medio de ordenador se ejecutaron por empleados de la misma empresa afectada. Otro estudio realizado en América Latina y Europa, indicó que el 73% de las intrusiones que se cometieron se atribuían a

[11]GDT - Grupo de Delitos Telemáticos. Disponible en: https://www.gdt.guardiacivil.es/webgdt/faq.php(consulta 14/05/2020).

[12] Qué es INCIBE | INCIBE. Disponible en: https://www.incibe.es/que-es-incibe(consulta 14/05/2020).

fuentes interiores, de modo que únicamente un 23% se atribuía a la actividad externa.[13]

2.3. SUJETO PASIVO DEL FRAUDE INFORMÁTICO

Debemos distinguir el sujeto pasivo o víctima del delito, sobre el cual recae la conducta de acción u omisión realizada por el sujeto activo, pudiendo ser en el caso de los delitos informáticos individuos, instituciones crediticias, gobiernos etc., los cuales hacen uso de sistemas automatizados de información que generalmente se encuentran conectados a otros.

Se debe puntualizar que, aunque la magnitud de estos delitos es alta, en el panorama mundial ha sido imposible tener conocimiento de la magnitud de los mismos, ya que en muchos casos los delitos no se descubren, o bien no se denuncian ante las autoridades responsables, faltando en muchos casos leyes que protejan a las víctimas de esos delitos. Las empresas por su parte, suelen evitar la denuncia de esta clase de conductas, por el temor al desprestigio que pueda causarles, así como las consecuentes pérdidas económicas, por lo que el índice estadístico de estas actuaciones se dice que se mantienen bajo la cifra oculta, o la cifra negra.[14]

---

[13] RAMÍREZ BEJERANO, EE. Y AGUILERA RODRÍGUEZ, AR. Los delitos informáticos. Tratamiento Internacional, Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm (consulta 20/04/2020).

[14] RAMÍREZ BEJERANO, EE. Y AGUILERA RODRÍGUEZ, AR. Los delitos informáticos. Tratamiento Internacional, Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm (consulta 20/04/2020).

2.4. FÓRMULAS DE FRAUDE INFORMÁTICO

En este apartado se analizarán las principales conductas ilícitas que se pueden llevar a cabo en Internet, y que son reconducibles al delito de estafa informática.[15]

2.4.1 Obtención de los datos o claves de acceso

2.4.1.1. Sustracción de las claves de acceso sin el conocimiento de la víctima

Nos referimos a la sustracción de las claves de acceso sin el conocimiento de las víctimas mediante el uso de *spyware*, programas que se introducen en el ordenador de la víctima sin su conocimiento para obtener datos que permiten suplantar la personalidad de la misma. La información que se trata de sustraer son claves bancarias, datos de tarjetas de crédito etc. Estos datos, una vez se envían al defraudador mediante conexión a la red, se utilizan para obtener un beneficio económico en favor del autor de la sustracción o bien de terceros.

Entre los *spyware* más conocidos encontramos los *troyanos*, aplicaciones que aparentan tener una función útil para el usuario, pero que realmente tienen una finalidad generalmente dañina. Cabe mencionar en relación a los *troyanos*, las *bombas lógicas*, que se diferencian de los primeros

---

[15] De acuerdo con MATA Y MARTÍN y GALÁN MUÑÓZ, si bien el robo de identidad encuentra su regulación en relación a la captación de los datos y la transferencia de los mismos a terceros en el artículo 197 del CP, la utilización de los datos no tiene regulación propia, sino que son la estafa y la estafa informática los tipos penales que permiten castigar las defraudaciones que se produzcan en caso de que exista engaño o manipulación informática, así como la más reciente estafa mediante tarjetas bancarias, en caso de que se traten de datos contenidos en tarjetas de crédito, débito o cheques de viaje. MATA Y MARTÍN, RM. Y GALÁN MUÑÓZ, A. Propuestas de política legislativa sobre el robo de identidad. En Cahiers de defense sociale, Numéro Extraordinaire á l`occasion du Duoziéme Congress des Nations Unies pour la prévention du crime et la justice pénale Salvador, Brésil, 2010, pp. 57-66, p.60.

en que mientras que los *troyanos* se activan cada vez que se ejecuta el programa, las *bombas lógicas* únicamente se activan en ciertas condiciones, como puede ser en una fecha determinada o con la apertura de un fichero con un nombre determinado. Esta clase de *spyware* suele introducirse en el ordenador mediante su descarga desde fuentes poco fiables o inseguras de internet o bien a través de la instalación de programas *freeware* o *shareware* que los contienen y mantienen ocultos.

Finalmente, cabe hacer mención a los *keyloggers*, que actúan mediante el registro de todo aquello que los usuarios teclean en su ordenador. Otros acceden a la información sin necesidad de que el usuario teclee nada, obteniendo los datos cuando el usuario ingresa en un enlace. [16]

2.4.1.2. Obtención fraudulenta de las claves (phishing)

Son aquellas conductas en las que la propia víctima sin saberlo facilita los datos necesarios para llevar a cabo transacciones al defraudador. [17]

Estas conductas se localizan en el ámbito de la estafa y consisten en la adquisición de información confidencial de manera ilícita, sin el consentimiento de su titular y haciendo uso de la ingeniería social, práctica mediante la cual se obtiene información confidencial a través de la manipulación de los usuarios legítimos. Por medio de esta práctica se pretende obtener información para llevar a cabo un acto perjudicial para un sujeto, o bien exponerlo a un riesgo o abuso. Por tanto, se entiende por *phishing* toda manipulación que se lleve a cabo con el fin de conseguir información privilegiada.

---

[16] FERNÁNDEZ TERUELO, JG. Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos en la red, en Revista de derecho penal y criminología 2ª Época, nº 19, pp. 217-243, pp. 218,219.

[17] SÁNCHEZ BERNAL, J. El bien jurídico protegido en el delito de estafa informática, en Cuadernos de Tomás nº 1, pp. 105-121, 2009, p. 106.

Respecto al autor del delito o *phisher*, puede simular ser una persona o empresa de confianza. Comete el hecho ilícito por medio de una comunicación electrónica aparentemente normal, como puede ser un correo electrónico, la mensajería instantánea, o bien mediante una llamada telefónica. El infractor que realiza la actividad delictiva frecuentemente simula ser la entidad bancaria con la que se encuentra vinculada la víctima o bien otros servicios que el sujeto pasivo tiene contratados logrando, mediante esta apariencia, conseguir los códigos, contraseñas, números de tarjetas y toda clase de información necesaria para llevar a cabo la estafa.[18]

Actualmente, los delincuentes que llevan a cabo esta clase de conductas (*phishers)* centran su actividad en el robo de datos personales, por medio de operaciones bancarias en línea como son la consulta de saldos, de transferencias, pagos por medio de Internet etc.

Respecto al papel del banco en este tipo de delitos, se ha pronunciado entre otras la Sentencia de la Audiencia Provincial (en adelante SAP) de Valencia 37/2017, de 25 de enero. [19]

El supuesto de hecho parte de que el acusado tenía el propósito de obtener un beneficio económico ilícito, mediante la transferencia de dinero a su cuenta bancaria desde varias cuentas de la víctima, cuyas claves de usuario y contraseñas había obtenido previamente. Finalmente, estas transferencias fueron bloqueadas por la entidad bancaria.

---

[18] SÁNCHEZ BERNAL, J. El bien jurídico protegido en el delito de estafa informática, en Cuadernos de Tomás nº 1, pp. 105-121, 2009, p.107.

[19] GARCÍA GARCÍA, DE. El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (REC. 1402/2016), en Rev. Boliv. de Derecho nº 25, pp. 650-659, p. 652.

La importancia de esta sentencia radica en que ofrece una amplia imagen acerca del concepto de *phishing*, centrándose en el *phishing bancario* como modalidad de estafa informática contenida en el artículo 248.2 a) del CP.

El *phishing bancario* se trata, de acuerdo con la Audiencia Provincial, de una técnica de ingeniería social que se caracteriza por el intento de obtener información confidencial de modo fraudulento. Supone, por tanto, la sustracción de datos bancarios por medio del uso de páginas web o bien mediante el envío de correos electrónicos con apariencia oficial, suplantando la identidad de las empresas o entidades de confianza, que con frecuencia se tratan de bancos.[20]

La Audiencia Provincial se retrotrae a la Sentencia del Tribunal Supremo (en adelante STS) de 2 de diciembre de 2014(RJ 845, 2014), que instaura un sistema de cuasi-responsabilidad civil objetiva de las entidades bancarias, basándose en la falta de diligencia del banco, al no disponer de las medidas de protección necesarias para el servicio de banca online. Esta argumentación supuso descartar el deber de autoprotección de la víctima, salvo cuando se trate de un engaño fácilmente identificable por cualquier persona.

Esto es debido a que la estafa informática se trata de un tipo delictivo complejo, que en muchos casos logra que la víctima no comprenda la intención real de la conducta delictiva, quedando incapacitada para reaccionar frente a ella. Es por tanto, un deber de la entidad bancaria el establecer las medidas necesarias frente a esta clase de delitos.[21]

De todo lo dicho hasta ahora cabe atribuir, en primer lugar, una responsabilidad penal por la comisión de la estafa informática al autor o autores

---

[20] GARCÍA GARCÍA, DE. El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (REC. 1402/2016), en Rev. Boliv. de Derecho nº 25, pp. 650-659, p. 654.

[21] GARCÍA GARCÍA, DE. El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (REC. 1402/2016), en Rev. Boliv. de Derecho nº 25, pp. 650-659, 2018, p. 655.

de la misma, así como a las personas que posibiliten la materialización del delito, que suelen denominarse *muleros.*

En segundo lugar, existe una responsabilidad civil cuasi-objetiva por la falta de diligencia de la entidad bancaria a la hora de adoptar las medidas necesarias para evitar la transferencia ilícita en favor del autor o autores del delito. Esta responsabilidad se deriva de la relación contractual existente entre la entidad bancaria, que provee el servicio de pago en línea, y el usuario que ha resultado estafado, conforme a la Ley 16/2009, de Servicios de Pago.

En la mayor parte de ocasiones en las que se producen esta clase de conductas delictivas, los tribunales se remiten a los artículos 31 y 32 de la Ley de Servicios de Pago para establecer un sistema de responsabilidad cuasi-objetiva de la entidad de crédito.[22]

El artículo 31 establece la responsabilidad del proveedor del servicio de pago en los supuestos de transferencias no autorizadas. Supone una obligación de restitución de la cuenta al estado anterior a la transferencia ilícita para la entidad bancaria que ofrece los servicios.

Sin embargo, el artículo 32 de la Ley de Servicios de Pago dispone que el usuario soportará en todo caso hasta un máximo de 150 euros de las pérdidas que se deriven de las transferencias no autorizadas en caso de que el instrumento de pago se haya extraviado o haya sido sustraído.

Únicamente responderá el usuario del total de las pérdidas, en caso de que sean fruto de una actuación fraudulenta, de incumplimiento deliberado o bien por negligencia grave de una o de varias obligaciones.

En el fallo de la SAP de Valencia se condena al acusado como autor de un delito de estafa informática en grado de tentativa, sin que quepa exigir responsabilidad civil contractual a la entidad bancaria por no haber adoptado las medidas de seguridad necesarias para evitar las transferencias

[22] GARCÍA GARCÍA, DE. El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (REC. 1402/2016), en Rev. Boliv. de Derecho nº 25, pp. 650-659, 2018, pp. 655-657.

fraudulentas, puesto que sí que las adoptó y logró bloquear dichas transferencias. [23]

Entre las modalidades de *phishing*, encontramos además el *pharming*. Supone la manipulación de direcciones DNS, que son aquellas que permiten acceder a los usuarios a las páginas web que quieren ver. El objeto de esta actuación es que las páginas visitadas no se correspondan con las auténticas, sino con otras cuya finalidad es la obtención de datos confidenciales, relacionados generalmente con la banca online.[24]

Las direcciones web de las páginas falsas suelen incluir un subdominio, como puede ser, por ejemplo, www.bancox.es.webdelphisher.es, o www.bancox.es@webdelphisher.es,que redirecciona a la página web que controla el *phisher* y no a la página web de la entidad bancaria que se desea acceder.

Esta modalidad de *phishing* es más fácil de detectar que la de *Cross Site Scripting*, [25] mediante la cual se hace uso del propio código del programa bancario, de forma que tanto la dirección web como los certificados de seguridad aparentan ser los originales de la entidad. Una vez el usuario entra en la página web, se le pide la confirmación de su cuenta, datos que serán posteriormente almacenados en la página web, permitiendo al *phisher* llevar a cabo el fraude.

---

[23] GARCÍA GARCÍA, DE. El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (REC. 1402/2016), en Rev. Boliv. de Derecho nº 25, pp. 650-659, 2018, pp. 655-657.

[24] FERNÁNDEZ TERUELO, JG. Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos en la red, en Revista de derecho penal y criminología 2.a Época, nº 19, pp. 217-243, 2007, p. 220.

[25]SÁNCHEZ BERNAL, J. El bien jurídico protegido en el delito de estafa informática, en Cuadernos de Tomás nº 1, pp. 105-121, 2009, p.108.

El modus operandi de las operaciones de *phishing* consiste normalmente en el envío de millones de mensajes de correo electrónico por el *phisher*, los cuales aun siendo falsos aparentan ser del sitio web de confianza del sujeto pasivo, pudiendo llegar a conocer incluso la entidad bancaria de la víctima y crear un señuelo personalizado. El defraudador incluye en muchas ocasiones vínculos falsos que permiten que la víctima acceda a un sitio web aparentemente legítimo, pero que ha sido creado por el *phisher.* Posteriormente, el individuo que ha sido engañado introduce las contraseñas, información de cuentas y otros datos personales necesarios para llevar a cabo el delito.

Finalmente, la información que ha sido introducida será remitida al infractor, el cual llevará a cabo el *phishing* en el momento en el que comience a retirar las cantidades de dinero de las cuentas, realice compras, solicite tarjetas de crédito etc. El capital será transmitido a los muleros, personas contratadas por una empresa ficticia y propietarios de cuentas bancarias que utilizan en su labor de intermediarios de la estafa, recibiendo una comisión por sus servicios. Los intermediarios, por último, transferirán el dinero a las cuentas bancarias de los autores de la conducta delictiva, que en la mayor parte de las ocasiones se encuentran a nombre de la supuesta empresa con la que han contratado, situada generalmente en paraísos fiscales, lo que posibilita el blanqueo de capitales.[26]

La conducta llevada a cabo por la mula a juicio FERNÁNDEZ TERUELO[27] se trata de una aportación idónea a la hora de fundamentar la imputación objetiva de una acción de cooperación necesaria o complicidad.

---

[26]SÁNCHEZ BERNAL, J. El bien jurídico protegido en el delito de estafa informática, en Cuadernos de Tomás nº 1, pp. 105-121, 2009, pp. 108 y 109.

[27] FERNÁNDEZ TERUELO, JG. Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos en la red, en Revista de derecho penal y criminología 2.a Época, nº 19, pp. 217-243, 2007, pp. 221 y 222.

Sin embargo, ha resultado problemática la determinación de la responsabilidad criminal de aquella persona que colabora en la comisión del hecho delictivo.

Una parte de la doctrina viene considerando que la conducta de los muleros se encuentra dentro del ámbito de la estafa informática, como cooperadores necesarios en la comisión del hecho delictivo.

Otro sector de la doctrina considera que la conducta de los muleros se trata de un delito de receptación como ocultación o encubrimiento de los efectos del delito, ya que lo que se trata es de evitar las sospechas de la entidad bancaria. El hecho de que la captación de los muleros puede producirse una vez se ha consumado el delito es lo que lleva a algunos autores a considerar que se trata más de un delito de receptación que un delito de estafa informática.

Por último, hay otros autores que consideran que estas conductas se encuadran dentro del delito de blanqueo de capitales.

Para la apreciación o no de la existencia de dolo eventual de la actuación que llevan a cabo los muleros, la Audiencia Provincial suele remitirse al concepto de ignorancia deliberada.[28]

2.4.2 Dialers

Los *dialers*, también denominados conexiones telefónicas fraudulentas, consisten en el uso de programas de marcado telefónico para establecer una conexión telefónica a redes, que implica una tarifa adicional de muy alto coste de la cual no se informa correctamente, o bien directamente se oculta. Es por ello que el uso de estos programas únicamente podrá ser lícito cuando se advierta de manera clara del coste que va a conllevar, así como las

[28] GARCÍA GARCÍA, DE. El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (REC. 1402/2016), en Rev. Boliv. de Derecho nº 25, pp. 650-659, 2018, p. 657.

modificaciones que van a llevarse a cabo en el sistema. Esta modalidad únicamente afecta a las conexiones mediante modem, mediante los sistemas RTB (red telefónica básica) o bien RDSI (red digital de servicios integrados), pero no a las conexiones por cable.[29]

2.4.3. Fraudes en el comercio electrónico

Son aquellos que se producen en la entrega de la cosa o el pago del precio. Las víctimas pueden ser tanto los consumidores como las empresas que se dedican al comercio, así como las entidades bancarias cuyos instrumentos de pago se entregan al vendedor.

La forma de comisión del fraude dependerá del sujeto pasivo del mismo, que puede ser el adquirente o bien el vendedor. En el primer caso, se produce la estafa mediante el envío o entrega de un bien que no posee las características por las cuales se llevó a cabo la adquisición. En el caso de que el fraude se cometa al vendedor, suele llevarse a cabo mediante la ausencia de pago o la suplantación del comprador real, cargándose la operación a un tercero ajeno a la misma. [30]

2.4.4. Envío de mails fraudulentos

En esta modalidad se hace uso del correo electrónico como medio o instrumento para el desarrollo de otros fraudes. Entre ellos encontramos la *estafa nigeriana*, que supone el envío masivo de emails en los que se ofrecen opciones para ganar dinero fácil mediante un desembolso inicial. Otras forma

---

[29] FERNÁNDEZ TERUELO, JG. Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos en la red, en Revista de derecho penal y criminología 2.a Época, nº 19, pp. 217-243, p. 222.

[30] FERNÁNDEZ TERUELO, JG. Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos en la red, en Revista de derecho penal y criminología 2.a Época, nº 19, pp. 217-243, p. 223.

de comisión del delito puede ser el envío de correos electrónicos en el que se informa a la víctima que se ha cargado una cantidad en una tarjeta de crédito, facilitando un teléfono con conexión internacional para posibles aclaraciones.[31]

2.5. FÓRMULAS DE ESTAFA MEDIANTE TARJETAS

2.5.1. Conductas llevadas a cabo mediante el uso ilícito de tarjetas

Entre las conductas que pueden llevarse a cabo mediante el uso ilícito de tarjetas como instrumento, encontramos la extracción ilegítima de dinero metálico en cajeros automáticos, la adquisición ilegítima de bienes o servicios mediante el uso de tarjetas en terminales de punto de venta y el pago no consentido por medio de redes informáticas. Todas estas conductas son reconducibles al artículo 248.2 c) del CP referido a la estafa mediante tarjetas de crédito, débito o cheques de viaje.[32]

2.5.1.1. Adquisición ilegítima de bienes o servicios en terminales de punto de venta (presencial)

En la estafa cometida mediante la presentación de la tarjeta en un comercio distinguimos los mismos elementos presentes en la estafa tradicional, a los cuales haremos referencia a posteriori en el trabajo.

En este sentido, debe de llevarse a cabo una conducta engañosa con ánimo de lucro por el autor de la estafa, que presenta la tarjeta al sujeto pasivo o comerciante, afirmando tener la capacidad de pago y solvencia necesaria.

---

[31] FERNÁNDEZ TERUELO, JG. Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos en la red, en Revista de derecho penal y criminología 2.a Época, nº 19, pp. 217-243, p.224.

[32] GARCÍA NOGUERA, I. La reforma penal de la falsificación, tráfico y uso ilícito de tarjetas bancarias en Revista de Internet, Derecho y Política, Universitat Oberta de Catalunya, p. 96.

Esta conducta engañosa tiene que ser suficiente para que se produzca una situación de error en el sujeto pasivo, que genere la confianza en la solvencia del que dice ser el titular de la tarjeta sin serlo realmente. [33]

Como consecuencia de la situación de error en el sujeto pasivo acerca de la recepción del pago, el comerciante lleva a cabo un acto de disposición patrimonial mediante la entrega de un bien o la prestación de un servicio. Finalmente, el acto de disposición patrimonial provoca un perjuicio patrimonial al comerciante, a la entidad emisora de la tarjeta o bien al titular de la misma. En el caso de que no se logre consumar la operación, la misma sería calificada como delito de estafa en el grado de tentativa, aplicándose lo dispuesto en el artículo 62 del CP.[34][35]

Se aprecia a su vez la necesidad por parte de la persona que recibe el pago de cumplir ciertos procedimientos a la hora de aceptarlo, es decir, desde el punto de vista de la producción del engaño suficiente es necesario que se cumplan ciertos requisitos de autoprotección a la hora de efectuar el pago, como son la verificación de que la tarjeta pertenece a la persona que la presenta al pago, así como la comprobación de la fecha de vencimiento de la misma.[36]

---

[33]JAVATO MARTÍN A.M. Las tarjetas de crédito y débito. Aspectos penales En Cuaderno Red de Cátedras Telefónica NO 10, Salamanca pp. 7,8 y 9.

[34] Art. 62 CP: A los autores de tentativa de delito se les impondrá la pena inferior en uno o dos grados a la señalada por la Ley para el delito consumado, en la extensión que se estime adecuada, atendiendo al peligro inherente al intento y al grado de ejecución alcanzado.

[35]JAVATO MARTÍN A.M. Las tarjetas de crédito y débito. Aspectos penales En Cuaderno Red de Cátedras Telefónica NO 10, Salamanca pp. 7,8 y 9.

[36] MATA Y MARTÍN RM Y JAVATO MARTÍN AM. Bank card fraud in Spain, En Digital Evidence and Electronic Signature Law Review Vol. 6, pp. 67-78, p.68.

2.5.1.2. Pago no consentido por medio de redes informáticas (no presencial)

La segunda de las modalidades de fraude con tarjetas bancarias es mediante el uso de medios electrónicos. La principal dificultad de este tipo de pago es la imposibilidad de presentar la tarjeta, no pudiendo por tanto llevar a cabo la comprobación de la firma del poseedor de la tarjeta, actuación requerida en el comercio presencial para lograr una mayor seguridad acerca de su titularidad. Es por ello, que deben de buscarse otros métodos para autentificar el pago, como puede ser la petición del código de validación de la tarjeta en el momento de llevar a cabo la compra a distancia.[37]

En las estafas realizadas haciendo uso de medios electrónicos, el autor lleva a cabo pagos por Internet mediante el uso indebido de los datos de una tarjeta ajena, a la que ha accedido anteriormente mediante el robo, hurto, clonación etc. A su vez, podrá el delincuente haber accedido a los datos de la tarjeta mediante la colaboración del comerciante o el establecimiento comercial, que pone a disposición del infractor el objeto necesario para llevar a cabo el delito.[38]

En los pagos ilícitos realizados por medio de las redes informáticas la jurisprudencia afirma que el engaño únicamente puede aparecer como un elemento personal entre dos sujetos. Lo mismo sucede con el error, el cual es consecuencia del acto engañoso y solo es posible en una relación entre personas. Es por ello, que tradicionalmente se ha reconducido este delito a la estafa informática (art. 248.2 a) CP).[39]

---

[37] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, p. 67.

[38] JAVATO MARTÍN A.M. Las tarjetas de crédito y débito. Aspectos penales En Cuaderno Red de Cátedras Telefónica NO 10, Salamanca, pp. 11-13.

[39] MATA Y MARTÍN RM Y JAVATO MARTÍN AM. Bank card fraud in Spain, En Digital Evidence and Electronic Signature Law Review Vol. 6, pp. 67-78, p.69.

2.5.1.3. Extracción ilegítima de dinero en cajeros automáticos

En esta clase de actuaciones, el sujeto activo hace uso de la tarjeta obtenida de manera ilícita para acceder a la máquina, que una vez introducido el número secreto pone a su disposición la cantidad de dinero que haya solicitado.[40]

2.5.2. Modalidades de estafa mediante tarjetas dependiendo de los métodos utilizados para su obtención

Para distinguir las clases de estafas que pueden llevarse a cabo por medio de tarjetas bancarias habrá de tenerse en cuenta, además del tipo de pago realizado, la actuación que ha llevado a cabo el delincuente para obtener la tarjeta de manera ilícita, la cual será utilizada atribuyendo un hecho y sus efectos jurídicos a una tercera persona. Estos efectos, abarcan desde los perjuicios meramente económicos hasta la posibilidad de que se produzca su detención.[41]

2.5.2.1. Carding

Esta modalidad de estafa supone el uso de una tarjeta bancaria de crédito o débito, o de cualquier otra que pueda emplearse como medio de pago como son las tarjetas de comercio o monedero electrónico. La tarjeta deberá haber sido obtenida por el infractor debido a su pérdida por el titular de la

---

[40] GARCÍA NOGUERA, I. La reforma penal de la falsificación, tráfico y uso ilícito de tarjetas bancarias en Revista de Internet, Derecho y Política, Universitat Oberta de Catalunya, p. 96.

[41] MATA Y MARTÍN, RM. Y GALÁN MUÓZ, A. Propuestas de política legislativa sobre el robo de identidad. En Cahiers de defense sociale, Numéro Extraordinaire á l`occasion du Duoziéme Congress des Nations Unies pour la prévention du crime et la justice pénale Salvador, Brésil, 2010, pp. 57-66, p.57.

misma, porque ésta haya sido sustraída a su propietario, o bien se haya obtenido por medio de engaño o fraude en el comercio tradicional.[42]

2.5.2.2. Skimming

Otra modalidad es el *skimming*, que supone el uso de una copia o reproducción de la tarjeta legítima. La copia total o parcial de la tarjeta posee los datos contenidos en la banda magnética de la tarjeta original, pudiendo usarse en la adquisición de bienes o servicios, así como para la extracción de dinero sin necesidad de desposeer al titular legítimo de la suya.[43]

En esta modalidad delictiva el delincuente se hace pasar por un representante de la empresa de servicios o banco con el que la víctima tiene suscrito un contrato, afirmando que debido a un problema debe verificar su cuenta por medio del correo electrónico, que supone una conducta de *phishing*. Si la comprobación se lleva a cabo por medio de una llamada telefónica. nos encontramos frente a un supuesto de *pretexting*, o bien *pharming* si se lleva a cabo mediante el desvío a páginas web falsas.

También podrán haberse obtenido los datos de las tarjetas por medio de programas rastreadores denominados *sniffers*, que se introducen en los ordenadores conectados a Internet en busca de la información que tengan almacenada, así como por medio del envío de SMS fraudulentos, técnica conocida como *smishing*.[44]

---

[42] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, p. 72.

[43] JAVATO MARTÍN A.M. Las tarjetas de crédito y débito. Aspectos penales En Cuaderno Red de Cátedras Telefónica NO 10, Salamanca pp. 19-22.

[44] MATA Y MARTÍN, RM. Y GALÁN MUÓZ, A. Propuestas de política legislativa sobre el robo de identidad. En Cahiers de defense sociale, Numéro Extraordinaire á l`occasion du Duoziéme Congress des Nations Unies pour la prévention du crime et la justice pénale Salvador, Brésil, 2010, pp. 57-66, p.58.

3. RESPUESTA INTERNACIONAL Y COMUNITARIA FRENTE A LA LUCHA CONTRA LA DELINCUENCIA INFORMÁTICA

3.1. LA UNIÓN EUROPEA ANTE LOS RIESGOS DE LAS NUEVAS TECNOLOGÍAS

La UE asume un papel importante a la hora de regular a nivel nacional los delitos sobre nuevas tecnologías, ya que al tener esta clase de fraudes un carácter fundamentalmente transfronterizo, es necesaria la creación de un ordenamiento supranacional.

El interés de la UE en este tipo de delitos parte de 1998, con la presentación de los resultados de un estudio sobre delincuencia informática(CONCRIME) por parte de la Comisión al Consejo. En él se daba a conocer la gran vulnerabilidad de la sociedad de la información, así como la gran cantidad de amenazas que provenían de nuevas tecnologías debido al desarrollo del comercio electrónico. Desde ese momento, la UE ha tratado de reforzar el mercado común europeo, convirtiéndose la seguridad electrónica en un requisito previo de gran importancia para el crecimiento electrónico y el correcto funcionamiento de la economía.[45]

Es por ello, que la UE se ha propuesto como objetivo principal en la materia, la aproximación de la legislación penal de los Estados miembros frente a ataques informáticos, para así lograr una mejor cooperación policial y judicial que permita una lucha más eficaz contra el terrorismo y la delincuencia organizada.

Entre las medidas adoptadas cabe mencionar, en primer lugar, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto

[45] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, pp.41 y 42.

de 2013, sobre Ataques a Sistemas de Información, que vino a sustituir la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005. Tiene como objetivo endurecer las penas del *hacking ilegal* y armonizar penalmente el tratamiento de los países de la UE frente a los ataques contra los sistemas de información. [46]

En materia de fraude informático debemos destacar la Directiva de la UE 2019/713 del Parlamento Europeo y del Consejo de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo, por la que se sustituye la Decisión marco 2001/413/JAI del Consejo. Esta Directiva,[47] surge como consecuencia de las lagunas y divergencias entre los Estados miembros en relación al ámbito del fraude y la falsificación de medios de pago distintos del efectivo, que dificultaban la persecución de esta clase de delitos. Por ello, el principal objetivo de la Directiva es recoger un compendio de medidas de Derecho penal que sean eficaces y eficientes para lograr la protección de los medios de pago que sean distintos del efectivo frente al fraude y la falsificación, siendo de aplicación tanto a los instrumentos de pago distintos del efectivo como a las monedas virtuales, que puedan usarse habitualmente para realizar pagos.

La Directiva, incluye normas mínimas sobre la definición de las infracciones penales, así como las sanciones aplicables en el ámbito del fraude y la falsificación de medios de pago distintos del efectivo. La Directiva define el

[46] Europa se refuerza penalmente frente a los ataques a los sistemas de Información | ECIJA. Disponible en: https://ecija.com/sala-de-prensa/europa-se-refuerza-penalmente-frente-a-los-ataques-a-los-sistemas-de-informacion/(consulta 29/05/2020).

[47] FERNÁNDEZ ROZAS, JC. Nuevas disposiciones de la Unión Europea sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Disponible en https://fernandezrozas.com/2019/05/15/nuevas-disposiciones-de-la-union-europea-sobre-la-lucha-contra-el-fraude-y-la-falsificacion-de-medios-de-pago-distintos-del-efectivo/(consulta 23/05/2020).

instrumento de pago distinto del efectivo como un dispositivo, objeto o registro protegido, material o inmaterial, o una combinación de ellos, excluyendo la moneda de curso legal, que actúa por si solo o bien por medio de un procedimiento o conjunto de procedimientos, permitiendo al titular o usuario la transferencia de dinero o valor monetario, incluso mediante instrumentos digitales de intercambio.

Entre las conductas sancionadas, la Directiva incluye formas clásicas como son el fraude, la falsificación, el robo o la apropiación ilícita. Aunque si bien es cierto, que al ser objeto de la Directiva los instrumentos de pago inmateriales, los define mediante la asimilación de las formas tradicionales y su correspondencia a la aplicación en la esfera digital, completando y reforzando en este sentido la Directiva 2013/40/UE del Parlamento y del Consejo.

En cuanto a las sanciones previstas, deberán de ser efectivas, proporcionadas y disuasorias en toda la UE. La regulación se caracteriza por establecer normas mínimas, en el sentido de que se otorga libertad a los Estados miembros (en adelante EEMM) para que adopten o mantengan una legislación penal más estricta sobre el fraude y la falsificación de medios de pago distintos del efectivo, así como poder incluir una definición más amplia de las infracciones. A su vez, impone penas más severas en caso de que el delito se haya cometido en el marco de una organización delictiva conforme a la Decisión marco 2008/JAI del Consejo.

Respecto a las normas de jurisdicción, se contempla que el Estado miembro deberá de adoptar las medidas necesarias frente a la infracción cuando esta haya sido cometida total o parcialmente dentro de su territorio, es decir, cuando el autor cometa la infracción estando físicamente en el territorio, o bien cuando el infractor se trate de uno de sus nacionales. [48]

[48] FERNÁNDEZ ROZAS, JC. Nuevas disposiciones de la Unión Europea sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Disponible en https://fernandezrozas.com/2019/05/15/nuevas-disposiciones-de-la-union-europea-sobre-la-

El intercambio de información sobre las infracciones contempladas en la Directiva se realizará mediante un punto de contacto nacional operativo que se encuentre disponible veinticuatro horas al día, durante los siete días de la semana. A su vez, los Estados miembros deben de poseer procedimientos para que las solicitudes de ayuda urgente se atiendan con rapidez, debiendo la autoridad competente responder a las mismas en un plazo de ocho horas desde la recepción.

Finalmente, en relación a la transposición de la directiva, se indica que los EEMM deben de adoptar las disposiciones legales, reglamentarias y administrativas que sean necesarias para el cumplimiento de lo establecido en la Directiva, fijando como fecha límite el 31 de mayo de 2021.[49]

3.1.1. Regulación en el derecho europeo de la estafa informática

En el Derecho europeo se estima que el delito de estafa informática debe de ser objeto de estudio vinculado con el delito de estafa tradicional. Sin embargo, existen opiniones divididas respecto al establecimiento de los límites de esa proximidad.

---

lucha-contra-el-fraude-y-la-falsificacion-de-medios-de-pago-distintos-del-efectivo/(consulta 23/05/2020).

[49] FERNÁNDEZ ROZAS, JC. Nuevas disposiciones de la Unión Europea sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo. Disponible en https://fernandezrozas.com/2019/05/15/nuevas-disposiciones-de-la-union-europea-sobre-la-lucha-contra-el-fraude-y-la-falsificacion-de-medios-de-pago-distintos-del-efectivo/(consulta 23/05/2020).

En Europa debe distinguirse entre los modelos que llevan a cabo una descripción exhaustiva de la estafa informática (Alemania y Portugal), frente a aquellos que hacen uso de definiciones generales (Italia y España).[50]

3.1.1.1. Regulación alemana

La estafa informática se encuentra regulada en Alemania en el § 263a del Código Penal Alemán, creada por el Art 1 de la Ley de lucha contra la criminalidad económica y ampliada mediante el artículo 1 Nº 10 de la 35ª Ley de modificación del derecho penal.

Se hace uso de un criterio restrictivo a la hora de aplicar el delito de estafa informática, correspondiéndose el comportamiento con un engaño a las personas, como sucede en el caso de la estafa tradicional. Es por ello, que únicamente se tendrá la conducta como estafa informática en aquellos casos en los que el uso de un proceso de tratamiento de datos sea relevante en la producción del perjuicio patrimonial, es decir, que sea consecuencia directa de la disposición patrimonial. Además, no se requeriría que el operador del sistema y el perjudicado sean los mismos, tratando el delito como defraudatorio y no de apropiación.[51]

La dificultad principal supuso hallar un equivalente análogo con el requisito de acción engañosa que causa el error y la disposición patrimonial en la actuación que se produce sobre un ordenador. La redacción final del precepto expone que el perjuicio patrimonial se produce al influir en el resultado

---

[50]BALMACEDA HOYOS, G. El delito de estafa informática en el derecho europeo continental, en Revista de derecho y ciencias penales nº 17, pp. 111-149, San Sebastián(Chile), p. 146.

[51] BALMACEDA HOYOS, G. El delito de estafa informática en el derecho europeo continental, en Revista de derecho y ciencias penales nº 17, pp. 111-149, San Sebastián(Chile), 2011, p. 113.

de una elaboración de datos, mediante la realización incorrecta de programas, haciendo uso de datos incorrectos o incompletos, el uso no autorizado de los mismos, o mediante una intervención ilícita.[52]

La primera de las actuaciones que tipifica el § 263 a), supone la incorrecta configuración del programa, entendido este como instrucciones de trabajo en un ordenador compuesto de una secuencia de comandos individuales, aunque no existe una respuesta acerca de qué se entiende como programa configurado correctamente.

El segundo de los ilícitos que contempla el artículo § 263 a) supone el uso de datos incorrectos o incompletos.

La tercera de las conductas que encontramos en este precepto es el uso no autorizado de datos. Es decir, se trata del uso de datos correctos por una persona no autorizada para ello.

La cuarta modalidad de comisión del delito consiste en cualquier otra forma de influencia no autorizada sobre el proceso. La falta de autorización es el elemento que constituye el contenido del injusto del comportamiento y una de las peculiaridades del delito.

Finalmente, el resultado típico supone que el hecho imponible tiene que influir en el proceso de tratamiento de datos informáticos. Es decir, la influencia de la actuación llevada a cabo por el autor debe provocar el cambio del resultado de los datos que se encuentran almacenados en el ordenador y de aquellos que son utilizados por el programa de trabajo.

Por todo ello, se puede concluir que la intención del legislador alemán es que el abuso de tarjetas bancarias, de otras tarjetas de código y

---

[52] RAMÍREZ BEJERANO, EE. Y AGUILERA RODRÍGUEZ, AR. Los delitos informáticos. Tratamiento Internacional, Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm (consulta 20/04/2020).

procedimientos de pago similares se deban de juzgar de modo acorde al § 263 a), al tratarse de la ley especial.[53]

3.1.1.2. Regulación italiana

En Italia, el delito de estafa informática se encuentra regulado en el artículo 640 ter del CP, añadido por el art. 10 de la Ley Nº 547 de 23/12/1993.

La doctrina italiana se inclina en su mayoría a afirmar que el tipo de estafa informática está inspirado en el delito de estafa tradicional, de modo que proponen el uso del artículo 640 únicamente en aquellos supuestos en los que el ordenador reemplace el proceso de toma de decisiones de la persona a la hora de valorar las situaciones relevantes desde la perspectiva económica. Por otro lado, se afirma que la simetría entre la estafa y la estafa informática no es perfecta, de modo que en la forma en la que se describe el tipo en el artículo 640 ter no se incluye el elemento de la inducción a error de la víctima. Este elemento, sin embargo, se considera implícito por el intérprete, para asegurar a la norma de la estafa informática un ámbito operativo que se encuentre circunscrito a las hipótesis en las que hubiera sido aplicable la norma de estafa tradicional si la conducta fraudulenta en lugar de dirigirse a un ordenador se hubiera dirigido a una persona.

El proceso por el cual se comete el delito de estafa informática en el ámbito del derecho italiano parte de la alteración del funcionamiento del sistema informático, o bien la intervención sin derecho sobre datos, informaciones o programas. En segundo lugar, se lleva a cabo la modificación del resultado regular del proceso de elaboración. Finalmente, se produce el provecho injusto con daño ajeno. Es decir, es necesario que se produzca una

[53] BALMACEDA HOYOS, G. El delito de estafa informática en el derecho europeo continental, en Revista de derecho y ciencias penales nº 17, pp. 111-149, San Sebastián(Chile), pp. 120-125.

consecuencia económica sobre la esfera patrimonial de la víctima, y que esta sea producto directo e inmediato del resultado que se altera en el proceso de elaboración.[54]

3.2. NORMATIVA INTERNACIONAL

Saliendo del ámbito de la UE, a nivel internacional se han producido una serie de resoluciones o propuestas sobre el tema, que han dado lugar a la modificación en ciertos casos de los derechos penales internacionales.[55]

Así, la Organización de Cooperación y Desarrollo Económico (OCDE) en 1986, procedió a publicar un informe que se titulaba Delitos de informática: análisis de la normativa jurídica, en el cual se reseñaban las normas legislativas que se encontraban vigentes, así como las propuestas de reforma de algunos Estados miembros, recomendándose una lista mínima de ejemplos de uso indebido, los cuales deberían de prohibir y sancionar las leyes penales de los EEMM.

A su vez, en 1992 la OCDE desarrolló una serie de normas para la seguridad de los sistemas de información, de modo que tanto los Estados como el sector privado pudieran establecer un mecanismo de seguridad para los sistemas informáticos. Mencionar, además, las Directrices que desarrolló la organización en 2002 para la Seguridad de Sistemas y Redes de Información.

Respecto a la Organización de Naciones Unidas (ONU), en el Octavo Congreso sobre Prevención del Delito de Justicia Penal celebrado en la

---

[54] BALMACEDA HOYOS, G. El delito de estafa informática en el derecho europeo continental, en Revista de derecho y ciencias penales nº 17, pp. 111-149, San Sebastián(Chile), p. 134.

[55] RAMÍREZ BEJERANO, EE. Y AGUILERA RODRÍGUEZ, AR. Los delitos informáticos. Tratamiento Internacional, Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm (consulta 20/04/2020).

Habana en 1990, que posteriormente seria recopilado en la resolución 45/121, de 14 de diciembre de 1990, se expuso que la delincuencia relacionada con la informática era consecuencia del aumento del uso del proceso de datos en los distintos países, aportando una descripción de los tipos de delitos informáticos y proponiendo modernizar las leyes nacionales de cada Estado, para que legislaran esta clase de delitos.

Debe mencionarse su vez el Manual de las Naciones Unidas para la Prevención y Control de Delitos informáticos de 1994, que expuso la dificultad añadida de que esta clase de delitos pasen a una esfera internacional, multiplicando los problemas, ya que se requiere una cooperación concertada entre los Estados.[56]

En el ámbito del Consejo de Europa cabe señalar la importancia del Convenio Europeo sobre Delincuencia Informática de Budapest de 20 de noviembre de 2001, sobre política penal común, del cual España fue parte desde sus inicios. Trató de armonizar aspectos que del Derecho penal material relacionados con conductas ilícitas por medios informáticos, encargándose a su vez de la política procesal común, de la competencia judicial y de la cooperación internacional. [57] Este Convenio establece una serie de grupos de infracciones que deben de incorporarse en las legislaciones nacionales y que se clasifican en cuatro grandes categorías de ilícitos, en cuyo segundo grupo de conductas encontramos los delitos informáticos, incluyendo la falsificación y el fraude informático.[58]

---

[56] RAMÍREZ BEJERANO, EE. Y AGUILERA RODRÍGUEZ, AR. Los delitos informáticos. Tratamiento Internacional, Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm (consulta 20/04/2020).

[57] DE LA CUESTA ARZAMENDI, J.L. Derecho penal informático. Navarra: Ed. Thomsons Reuters, p. 124.

[58] MATA Y MARTÍN RM Y JAVATO MARTÍN AM. Bank card fraud in Spain, En Digital Evidence and Electronic Signature Law Review Vol. 6, pp. 67-78, p.74.

Finalmente, cabe destacar dos encuentros relevantes para los delitos informáticos en el ámbito internacional. En 1992, la Asociación Internacional de Derecho Penal durante el coloquio que se celebró en Wurzburgo, adoptó una serie de recomendaciones respecto a los delitos informáticos. Entre ellas destaca una propuesta realizada en la que se afirma que en la medida en que el Derecho Penal actual no sea suficiente, se deberá promover la modificación de la definición de los delitos existentes, o bien la creación de otros nuevos en caso de que no baste con otras medidas, como pueden ser la aplicación del principio de subsidiariedad.

A su vez, debe de hacerse referencia a las Segundas Jornadas Internacionales sobre el Delito Cibernético en Mérida en 1997, en las que se desarrollaron temas como la aplicación y administración de las tecnologías Informáticas, el papel de la cibernética en el blanqueo de capitales, el contrabando y narcotráfico, el establecimiento de una policía europea para la persecución del delito cibernético etc.[59]

4. ANÁLISIS DE LAS PRINCIPALES CONDUCTAS DELICTIVAS

4.1. LA ESTAFA TRADICIONAL

Para facilitar la comprensión de la estafa informática y la estafa cometida mediante el uso de tarjetas, se debe de hacer referencia al delito de estafa que suele recibir el apelativo de tradicional, analizando sus elementos integrantes.

---

[59] RAMÍREZ BEJERANO, EE. Y AGUILERA RODRÍGUEZ, AR. Los delitos informáticos. Tratamiento Internacional, Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm (consulta 20/04/2020).

Este delito se encuentra tipificado en el artículo 248.1 del CP. De acuerdo con la definición dada por ANTÓN ONECA[60], se trata de "la conducta engañosa, con ánimo de lucro injusto, propio o ajeno, que, determinando un error en una o varias personas, les induce a realizar un acto de disposición, a consecuencia del cual se produce un perjuicio en su patrimonio o en el de un tercero".

Los elementos del tipo se establecen en el contexto de relaciones causales entre ellos, que parten de la producción de engaño por el autor, que lleva a originar un error que hace que el engañado lleve a cabo un acto de disposición que le produce un perjuicio patrimonial. A lo largo de toda la estafa el delincuente deberá actuar además con ánimo de lucro.[61]

4.1.1. Elementos de la estafa tradicional

4.1.1.1. Engaño

El primero de los elementos objetivos de la estafa es el engaño, que se trata del desvalor de la acción del delito. En la estafa, el autor hace uso de un procedimiento fraudulento para lograr el engaño de la víctima, siendo la base fundamental del hecho punible. Es definido por ANTON ONECA[62] como "la falta de verdad en lo que se dice o hace, de manera suficiente para inducir a error".

El engaño deberá ser suficiente para producir error en otras personas, por lo que hay conductas que no llegan a ser típicas o espacios de riesgo permitido. Además, en la estafa se requiere una observación suficiente de veracidad y autoprotección. No existirá engaño si se llevó a cabo una conducta

---

[60]ANTÓN ONCECA, J.. Estafa, en Nueva Enciclopedia jurídica, Tomo IX (dir. MASCAREÑAS Carlos-E), Ed. Franciso Seix SA, pp. 56 y ss., Barcelona, p.89.

[61]MATA Y MARTÍN RM. Comentarios prácticos al código penal, Navarra, p.166.

[62]ANTÓN ONCECA, J. Estafa, en Nueva Enciclopedia jurídica, Tomo IX (dir. MASCAREÑAS Carlos-E), Ed. Franciso Seix SA, pp. 56 y ss., Barcelona, pp. 67 y ss.

tosca o burda por el estafador, que debió de haber sido detectada por el perjudicado, en atención a sus circunstancias personales.[63]

4.1.1.2. Error

El segundo de los elementos es el error, consecuencia directa del engaño, que supone el conocimiento viciado o inexacto de la realidad.

En aquellos supuestos que la víctima duda acerca de la veracidad de la conducta del autor, se cuestiona la existencia de error. Es por ello, que para la jurisprudencia la existencia de un error esencial en el sujeto pasivo es un elemento necesario para que se produzca el delito de estafa.[64]

4.1.1.3. Acto de disposición patrimonial

En tercer lugar, debe de producirse un acto de disposición patrimonial. Se trata del resultado típico de la estafa, que nos permite diferenciar la estafa del hurto, en aquellos casos en los que se produce una apropiación de cosas muebles mediante el engaño por parte del autor.[65]

Este acto puede afectar a cualquier elemento patrimonial, concretándose en una actuación por el engañado en la que entrega una cosa, realiza un acto documental económico o presta alguna clase de servicio que sea cuantificable de forma económica.[66]

4.1.1.4. Perjuicio patrimonial

El cuarto elemento, consecuencia inmediata del acto de disposición patrimonial, es la producción de un perjuicio patrimonial para quien sufre el

---

[63]MATA Y MARTÍN RM. Comentarios prácticos al código penal, Navarra, pp.168 y 169.

[64] MATA Y MARTÍN RM. Comentarios prácticos al código penal, Navarra, pp.168 y 169.

[65] CHOCLÁN MONTALVO, J.A. El delito de estafa. Nº 2. Barcelona. Ed. Bosch, pp.186-188.

[66] MATA Y MARTÍN, RM. Comentarios prácticos al código penal, Navarra, p.170.

comportamiento engañoso, o bien un tercero.[67] Por lo tanto, no es necesario que coincidan ambos sujetos, pudiendo ser el engañado y el perjudicado patrimonialmente personas distintas.[68]

4.1.1.5. Ánimo de lucro y dolo

Se trata de un elemento existente en la esfera interna del autor que debe de concurrir con los elementos objetivos anteriormente señalados. El ánimo de lucro y dolo suponen la búsqueda del enriquecimiento injusto económico del autor, la intención de lograr un beneficio patrimonial para sí mismo.[69]

4.1.1.6. Nexo causal

Todos los elementos señalados, deberán de estar unidos por un nexo causal que relaciona el engaño y el perjuicio. El engaño debe motivar el error que causa el acto de disposición patrimonial que produce finalmente el perjuicio patrimonial en la víctima.[70]

4.1.2. Pena

La pena contemplada en el artículo 249 del CP, así como los agravantes que se recogen en los artículos 250 y 251, son de aplicación tanto a la estafa tradicional o convencional (artículo 248.1 CP), como a las modalidades de estafa informática y estafa mediante tarjetas bancarias (art. 248.2 a) y c) CP).

En este sentido, la pena contemplada en el artículo 249 del CP para los delitos de estafa es de prisión de 6 meses a 3 años, teniéndose en cuenta para establecer la pena las circunstancias en las que se cometió el delito de estafa.

---

[67] PÉREZ MANZANO, M. Acerca de la Imputación Objetiva de la Estafa, en hacia un Derecho Penal Económico Europeo, Universidad Autónoma de Madrid, pp. 285-309, Madrid, p. 303.

[68] MATA Y MARTÍN RM. Comentarios prácticos al código penal, Navarra, p.171.

[69] MATA Y MARTÍN RM. Comentarios prácticos al código penal, Navarra, p.171.

[70] MATA Y MARTÍN RM. Comentarios prácticos al código penal, Navarra, p.171.

El segundo párrafo añade que en caso de que la cuantía de lo defraudado no supere los 400 euros, la pena va a ser de multa de 1 a 3 meses.

Por tanto, los criterios que se observan para establecer la pena de este delito son, que en caso de que el importe defraudado no sea superior a 400 euros, se establece pena de multa, mientras que, si la cantidad estafada excede de 50000 euros, se aplicará la pena agravada del artículo 250 del CP. En relación a las circunstancias en las que se cometió el delito de estafa, el precepto se refiere al quebranto económico que se causa al perjudicado, así como las relaciones existentes entre el autor y la víctima atendiendo a si el autor se aprovechó de su relación con el sujeto pasivo para cometer la estafa. Por último, deberán valorarse a su vez los medios empleados por el autor, variando la pena dependiendo de su mayor o menor gravedad.[71]

Respecto de los agravantes del artículo 250 y 251 del CP, no serán objeto de análisis del presente trabajo. Únicamente mencionar, que el artículo 250 contempla penas de prisión de uno a seis años y multa de seis a doce meses para aquellas estafas en las que concurran una serie de circunstancias, mientras que el artículo 251 contempla pena de prisión de uno a cuatro años si se dan los requisitos previstos en el precepto.

4.2. LA ESTAFA INFORMÁTICA

El delito de estafa informática se introdujo en el Código penal de 1995 como consecuencia de la existencia de una laguna legal, al no poderse aplicar a esta clase de comportamientos delictivos defraudatorios informáticos el tipo clásico de estafa, ya que ésta debía de llevarse a cabo de modo personal,

[71] FERNÁNDEZ MORÓN, A. Aspectos esenciales del delito de estafa en el Código Penal español, Universidad de Alcalá, pp. 46 y 47.

siendo uno de sus elementos el engaño. En este sentido, la doctrina afirmaba "que las máquinas no pueden ser engañadas".[72]

Se regula en el artículo 248.2 a) del CP, castigando la manipulación de datos sobre sistemas informáticos con el fin de conseguir una transferencia no consentida de activos patrimoniales.

No son objeto de regulación en este precepto aquellas estafas comunes que hayan sido cometidas en la red, sino aquellas estafas cometidas por medio de manipulaciones informáticas, manipulaciones en el proceso de elaboración electrónica de cualquier clase y en cualquier momento, que tengan como finalidad la obtención de un beneficio económico que cause a un tercero un perjuicio patrimonial.[73]

En este sentido, la manipulación informática es definida por ROMEO CASABONA como cualquier acción volcada tanto sobre los datos procesados automáticamente como a las instrucciones del programa, interviniendo en el sistema y causando como efecto la alteración o modificación del resultado correcto del tratamiento informático.[74]

GALÁN MUÑOZ señala que la manipulación informática puede darse en momentos distintos. Puede producirse en la entrada de datos, introduciendo datos falsos o bien provocando la alteración, supresión u ocultación de los ya introducidos.[75]

---

[72] FERNÁNDEZ TERUELO, JG. Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos en la red, en Revista de derecho penal y criminología 2.a Época, nº 19, pp. 217-243, p. 234.

[73] BALMACEDA HOYOS, G. El delito de estafa informática en el derecho europeo continental, en Revista de derecho y ciencias penales nº 17, pp. 111-149, pp. 135.

[74] ROMEO CASABONA, CM. Delitos informáticos de carácter patrimonial, en Revista iberoamericana de derecho informático, nº 9-11, pp. 413-442, p. 417.

[75] GALÁN MUÑOZ, A. El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 CP, Valencia, p. 556 y 559.

Además, podrá producirse la manipulación en el programa en la fase de tratamiento de los datos, lo que supone la alteración de las instrucciones que constituyen el programa, para que actúe de forma distinta a su configuración, permitiendo al autor obtener los datos correctamente introducidos[76]. El autor podrá obtener a su vez los datos mediante modem, red etc., por lo que no es necesario que tenga contacto directo con el ordenador de la víctima.

4.2.1. Bien jurídico protegido

El bien jurídico protegido mediante la tipificación penal se trata de un elemento fundamental a la hora de determinar su naturaleza, extensión, límites y alcance de la protección que ofrece, permitiendo calificar de típica o atípica una conducta concreta. Se trata de lograr aclarar el interés socialmente protegido o el valor relevante para, en caso de que se vulnere, se imponga el castigo correspondiente.[77]

Los nuevos tipos penales que sancionan conductas que atentan contra una variedad de bienes jurídicos haciendo uso de los medios informáticos, tecnologías telemáticas e Internet han sido agrupados por la doctrina dentro del concepto de delitos informáticos, que abarca todas aquellas conductas criminales realizadas por medio de ordenador y que afectan al funcionamiento de los sistemas informáticos.[78]

Sobre el bien jurídico protegido por el tipo penal de estafa informática se han sostenido diversas teorías.

En primer lugar, se considera que el bien jurídico protegido por la estafa informática es el patrimonio, debiendo de señalarse tres concepciones de

---

[76] CHOCLÁN MONTALVO, J.A. El delito de estafa. Nº 2. Barcelona, p.328.

[77] SÁNCHEZ BERNAL, J. El bien jurídico protegido en el delito de estafa informática, en Cuadernos de Tomás nº 1, pp. 105-121, p. 109.

[78]. PÉREZ LUÑO AE. Manual de Derecho Informático y Derecho, Barcelona, p. 69.

patrimonio: una jurídica, en la que el patrimonio se entiende desde la perspectiva del derecho objetivo, como el conjunto de derechos subjetivos patrimoniales de una persona; otro económica, que engloba aquellos valores económicos que una persona posee de hecho; y finalmente una económico-jurídica, que considera el patrimonio como aquél conjunto de bienes y derechos patrimoniales económicamente evaluables que posee un sujeto por medio de una relación que reconoce el ordenamiento jurídico.

Sin embargo, encontramos cierta controversia acerca del bien jurídico protegido por la estafa informática entre la tesis de la propiedad y la tesis del doble bien jurídico protegido.

A finales del s. XX, la mayoría de la doctrina consideraba que el patrimonio era el único bien jurídico protegido por la estafa electrónica, incluyendo en este concepto tanto bienes muebles e inmuebles como derechos reales y de crédito. Otros autores, aunque de manera minoritaria, consideraban que junto al ataque contra los elementos patrimoniales debía de producirse la disminución económica del patrimonio.[79]

Por último, encontramos la teoría del bien jurídico intermedio, defendida por GALÁN MUÑOZ [80], que considera el delito de estafa informática como un delito de peligro-lesión. Niega la necesidad de interpretar de manera vinculada el delito de estafa tradicional con el delito de estafa informática. Es por ello que afirma que en la estafa informática no se protegen únicamente bienes jurídicos individuales, sino también colectivos, debiendo de incluirse dentro de los delitos económicos en sentido amplio.

Por tanto, si se considera que la estafa informática se trata de un delito que protege valores económicos supraindividuales, serían dos los bienes

---

[79] SÁNCHEZ BERNAL, J. El bien jurídico protegido en el delito de estafa informática, en Cuadernos de Tomás nº 1, pp. 105-121, 2009, pp. 116 y 117.

[80] GALÁN MUÑÓZ A., El fraude y la estafa mediante sistemas informáticos, Valencia, pp.197 y ss.

jurídicos que se lesionan. El primero sería el patrimonio, que a su vez pone en peligro otro bien jurídico de naturaleza colectiva, que es el correcto funcionamiento de determinados sistemas informáticos.

En este sentido, la introducción de un bien jurídico intermedio legitima para un sector de la doctrina la introducción de la técnica del peligro abstracto en los delitos económicos. Esta postura es criticada por algunos autores, que entienden que otorgar relevancia penal a la simple puesta en peligro del bien jurídico colectivo supondría castigar comportamientos alejados de la ejecución de la conducta que realmente perturba el bien jurídico.

Finalmente, cabe concluir de conformidad con la opinión mayoritaria de la doctrina, que el bien jurídico protegido por el delito de estafa informática es el patrimonio, entendiéndose de forma amplia como conjunto de derechos, bienes y relaciones jurídicas de las que puede ser titular un sujeto. [81]

4.2.2. Elementos estafa informática

4.2.2.1. Diferencias entre estafa común del artículo 248.1 del CP y la estafa informática del artículo 248.2 del CP.

Las características de la estafa informática difieren en algunos elementos frente a la estafa común. En este sentido, la estafa informática se llevará a cabo valiéndose además del engaño o error, de alguna manipulación informática o artificio semejante. Es por ello que, al proteger este tipo delictivo el patrimonio frente a los actos llevados a cabo por medio de una manipulación informática o artificio semejante, el engaño, elemento esencial de la estafa tradicional, pasa a un segundo plano en la estafa informática. [82]

---

[81]SÁNCHEZ BERNAL, J. El bien jurídico protegido en el delito de estafa informática, en Cuadernos de Tomás nº 1, pp. 105-121, pp. 118-121.

[82] SSTS nº 533/2007, de 12 de junio, FD Segundo: Sobre la inexistencia de engaño por parte de los recurrentes, sólo recordar que, dada la estructura de la estafa informática, y

Respecto al error, no se trata de un requisito necesario en la estafa informática, ya que el desplazamiento que se produce como consecuencia de la manipulación informática, se realiza en relación a un programa informático y no a un sujeto, por lo que no puede concurrir este elemento. [83]

4.2.2.2. Transferencia no consentida de activos patrimoniales

El resultado de la manipulación informática del autor de la estafa informática es la realización de una transferencia en perjuicio patrimonial de un tercero, guiándose el autor por ánimo de lucro.[84] Este requisito se trata del equivalente al acto de disposición de la estafa tradicional. [85]

El ánimo de lucro se entiende de forma distinta a la estafa clásica, en la que consiste en la actuación que se realiza con la intención de obtener un beneficio económico para sí o para un tercero. Por el contrario, en la estafa informática supone que el autor pretende provocar una transferencia de activos patrimoniales ajenos por medio de manipulaciones informáticas que le lleven a obtener un beneficio económico.[86]

La actuación que se castiga es la transferencia no consentida de activos patrimoniales, entendidos como bienes muebles e inmuebles. A sensu

---

estamos en una estafa cometida a través de una transferencia no consentida por el perjudicado mediante manipulación informática, en tales casos no es preciso la concurrencia de engaño alguno por el estafador.

[83] SSTS nº 1476/2004, de 21 de diciembre, FD Primero: 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 responde al esquema típico del art. 248.1 CP, pues no se dirigen contra un sujeto que pueda ser inducido a error.

[84] MATA Y MARTÍN RM. Comentarios prácticos al código penal, Navarra, pp.172 y 173.

[85] BALMACEDA HOYOS G. El delito de estafa informática en el derecho europeo continental, En Revista de derecho y ciencias penales Nº 17, San Sebastián(Chile), pp. 111-149, p. 139.

[86] GALÁN MUÑOZ, A. El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 CP, Valencia, p. 790.

contrario, no se castigan aquellas conductas que no resulten en esta operación.[87]

GALÁN MUÑÓZ[88] afirma que la ausencia de consentimiento de la transferencia deberá de probarse positivamente, no siendo suficiente la afirmación de la imposibilidad de constatar su presencia, ya que si lo fuese se trataría de una presunción iuris tantum contraria al principio de presunción de inocencia. Si no se dispone de prueba acerca de la ausencia de consentimiento, el comportamiento es atípico.

Además, la sola transferencia no consentida de los activos no supone la realización del tipo, ya que este no se consumará hasta que no se logre el efectivo perjuicio de un tercero como consecuencia de la transferencia.[89] Por tanto, el resultado consumativo ha de ser necesariamente el perjuicio patrimonial de un tercero, debiendo de ser real, efectivo y evaluable económicamente.

4.2.2.3. Manipulación informática o artificio semejante

La transferencia no consentida del activo patrimonial deberá llevarse a cabo por medio de manipulación informática o artificio semejante. Sin embargo, lo relevante en este tipo penal no es tanto que la transferencia de los activos se realice por medio de instrumentos informáticos, ni que se haga uso de ellos

[87]GARCÍA GARCÍA-CERVIGÓN, J. El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico, en Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales nº 74, pp. 289-308, p. 296.

[88] GALÁN MUÑOZ, A. El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 CP, Valencia., pp. 644 y 646.

[89] CHOCLÁN MONTALVO, J.A. El delito de estafa. Nº 2. Barcelona, pp.338-348.

para encubrir apoderamientos por otros medios, sino que la propia manipulación del autor se lleve a cabo por medios informáticos.[90]

Por manipulación informática se entiende, de acuerdo a la Decisión marco 2001/413/JAI del Consejo, toda actuación que recaiga sobre un sistema informático y suponga la introducción de datos falsos, la introducción indebida de datos reales, la manipulación de aquellos datos que se contengan en el sistema informático durante cualquier fase del tratamiento y las interferencias que afecten al sistema o al programa.

Algunos definen de manera amplia la conducta típica que se realiza en la manipulación informática como todas aquellas operaciones que supongan un incorrecto uso o bien provoquen un incorrecto funcionamiento de un sistema de procesamiento de datos. Esta teoría considera el sistema informático como mero instrumento o medio de ejecución de la estafa informática, siendo contraria a aquellas otras tesis que comparan el papel del sistema informático con el de la víctima del engaño de la estafa informática y que suponen la "humanización de los ordenadores".[91]

Cabe mencionar que no entrarían dentro de la calificación de estafa informática aquellas manipulaciones informáticas, enfocadas a eludir el pago de las contraprestaciones, que se realicen en el ámbito de los servicios de telecomunicaciones, ya que no suponen una transferencia de activos patrimoniales, sino el impago del crédito que se genera por el servicio prestado. Tampoco se considerará manipulación informática la destrucción de datos en

---

[90] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, p.100.

[91] GALÁN MUÑOZ, A. El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 CP, Valencia, pp. 571, 574, 583, 586 y 688.

un sistema informático de una entidad bancaria, ya que en ese caso se trata exclusivamente de daños informáticos.[92]

Por otro lado, la mención que realiza el precepto a un artificio semejante supone que el tipo es considerado como un delito de resultado, ya que se exige únicamente el uso de algún artificio informático o similar.[93]

El legislador español a la hora de establecer la expresión de artificio semejante pretendía poder castigar también las manipulaciones de máquinas automáticas que proporcionan servicios y mercancías y que no podían ser consideradas informáticas en el caso concreto. Esta actuación legislativa fue criticada, ya que la obtención por medios fraudulentos de esta clase de prestaciones no es equiparable a la manipulación informática.

La dificultad de delimitar el alcance del artificio semejante, ha llevado a adoptar posturas en las que se acoge una doble interpretación como puede ser "artificio semejante a la manipulación" o "artificio semejante no informático". De acuerdo con BALMACEDA HOYOS[94], lo más correcto sería realizar una interpretación amplia, calificando el artificio semejante como informático y estudiándose de manera conjunta a la manipulación informática, evitando de este modo la casuística y salvaguardando la seguridad jurídica y el principio de legalidad.

En este sentido, debe tenerse en cuenta que la obtención fraudulenta de bienes o servicios de una máquina automática o por medio de manipulación mecánica no guarda relación con la manipulación de un sistema informático,

---

[92] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, p.107.

[93] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, p.89.

[94] BALMACEDA HOYOS G, El delito de estafa informática en el derecho europeo continental, En Revista de derecho y ciencias penales No 17, San Sebastián(Chile), pp. 111-149, pp. 138 y 139.

por lo que se reduce la interpretación extensiva del concepto de artificios semejantes utilizado por el legislador. [95]

4.2.3. Sujetos de la estafa informática

En la estafa informática debe de haber dos sujetos, uno que engaña con dolo y ánimo de lucro y otro que es engañado, viendo perjudicados sus intereses.[96] La inexistencia de dolo por el autor del delito supone que no tuvo intención de provocar mediante el engaño ninguna clase de disposición patrimonial perjudicial.

El sujeto activo puede tratarse de cualquier persona, mientras que el sujeto pasivo deberá ser aquel perjudicado patrimonialmente por un acto de disposición ejecutado por él mismo o por un tercero como consecuencia del engaño.

Respecto a la posibilidad de que un sujeto pueda calificarse como autor de la estafa informática por comisión por omisión, GALÁN MUÑOZ [97] afirma que para que se dé esta posibilidad, el sujeto debería de estar en una posición de garante respecto a la generación del perjuicio patrimonial que se deriva de la transferencia informática de activos patrimoniales ajenos y no respecto al funcionamiento o resultado del proceso que se lleva a cabo por medio del sistema informático. Por tanto, el autor solamente asumirá las funciones de proteger el bien jurídico cuando tenga un deber de lealtad o fidelidad respecto al patrimonio del tercero.

---

[95] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, p.99.

[96]PÉREZ MANZANO, Mercedes. Las defraudaciones (I). Las estafas, en Comprendido de Derecho Penal Parte Especial Volumen II (dir. BAJO FERNÁNDEZ Miguel), pp. 447 y ss., Madrid, pp. 451 y ss.

[97] GALÁN MUÑOZ, A. El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 CP, Valencia, pp. 653-655.

Continúa el autor exponiendo que, si el sujeto no se encuentra en la posición de garante, únicamente adquieren el deber de evitar el resultado típico cuando su actuación ponga en peligro el bien jurídico mediante la injerencia, siempre y cuando la creación o incremento del riesgo no se haya producido por medio de la actuación dolosa del autor. Este sería el caso en el que el sujeto pudo haber evitado el resultado y no lo hizo, habiendo asumido previamente funciones de protección del bien jurídico.

La admisibilidad de la comisión por omisión en la estafa informática es controversial entre la doctrina[98], aunque HERRERA MORENO[99] señala que es posible que se produzca en el ámbito de la ocultación de datos en relación a la manipulación informática, ya que se trata de una conducta activa que se produce mediante actuaciones como son la presión de una tecla para ocultar de manera positiva que los datos que tienen que ser conocidos se muestren en el ordenador. Sin embargo, la simple ocultación omisiva es cuestionada por la autora en relación al cumplimiento de la exigencia recogida en el artículo 11 del CP acerca de la omisión impropia, señalando que la conducta consciente de ocultación que supone la omisión de los datos que deben de exteriorizarse supone el origen de la posición de garante del autor. En este sentido se encuentra a su vez de acuerdo MATA Y MARTÍN[100], ya que considera que si se admite como manipulación informática la no inclusión de los datos reales que tienen que ser objeto de procesamiento, se estaría produciendo una omisión.

---

[98] DEVIA GONZÁLEZ, EA. Delito informático: Estafa Informática del artículo 248.2 del Código Penal (dir. POLAINO NAVARRETE Miguel), Universidad de Sevilla, pp. 306-308.

[99] HERRERA MORENO, M. El fraude informático en el derecho penal español. En Revista de Actualidad Penal nº 39, Sevilla, pp. 954 y ss.

[100] MATA Y MARTÍN, RM. Delincuencia informática y Derecho Penal, Madrid, p. 54.

4.2.4. Lugar de comisión del delito y competencia jurisdiccional

Se plantea el problema de la determinación del lugar de comisión del delito, ya que los delitos informáticos se caracterizan normalmente por encontrarse el autor en un lugar, la víctima del delito en un segundo y el hecho delictivo en un tercero.[101] Este problema se une al carácter supranacional que tienden a tener esta clase de delitos, viéndose normalmente involucrados dos o más países.

El TS viene decantándose por el principio de ubicuidad, es decir, que el delito se comete en todas las jurisdicciones territoriales en las que se realice alguno de los elementos del tipo. Conocerá por tanto del delito aquel juez que inicie las actuaciones, que será competente para la instrucción de la causa.[102]

Por otro lado, el Convenio de Budapest de 23 de noviembre de 2001 viene utilizando el principio de territorialidad, es decir, conocerá el Estado de los delitos informáticos cometidos en su territorio[103].

---

[101] PÉREZ MACHÍO, AI. Dos problemas particulares de cara a la persecución de los delitos informáticos, en Derecho penal informático (dir. DE LA CUESTA ARZAMENDI JL/ coord. DE LA MATA BARRANCO NJ), pp. 247-277, 2010.

[102] Acuerdo Sala General TS de 3 de febrero de 2005.

[103] Artículo 22 del Convenio sobre la ciberlincuencia. Budapest, 23 de noviembre de 2001 1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido: a) En su territorio; o b) a bordo de un buque que enarbole pabellón de dicha Parte; o c) a bordo de una aeronave matriculada según las leyes de dicha Parte; o d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

4.3. LA ESTAFA MEDIANTE LA UTILIZACIÓN DE TARJETAS BANCARIAS.

4.3.1. Antecedentes

4.3.1.1. Hurto y robo con fuerza sobre las cosas

En un principio, la Decisión marco 2001/413/JAI del Consejo, de 28 de mayo sobre lucha contra el fraude y la falsificación expuso en el artículo 2 que los Estados miembros debían de adoptar las medidas que fueran necesarias para calificar de delitos, al menos respecto a su comisión con tarjetas de crédito, aquellos casos en los que se produjera de forma deliberada el uso fraudulento de instrumentos de pago que hayan sido objeto de robo u otra forma de apropiación indebida, falsificación o manipulación.

Por tanto, la discusión giraba en torno al uso de tarjetas ajenas, obtenidas de manera ilícita, por error, por haber sido encontradas o bien por abuso de la confianza del titular legítimo, con finalidad de extraer dinero del cajero automático.[104] En este sentido, el hecho de que los cajeros automáticos se encontrasen localizados en un espacio cerrado y que fuese necesaria la tarjeta del banco para obtener acceso, llevó a los tribunales a calificar este delito como robo mediante uso de llaves falsas.[105]

En el pasado ya había sido resuelta una problemática similar como fue la calificación del empleo de tarjetas magnéticas o perforadas, utilizadas entre otros en hoteles, o en mandos de apertura a distancia. La solución la recogió el CP de 1995, en el artículo 239 inciso final del CP[106], que las consideró como

---

[104] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, pp. 51 y 52.

[105] MATA Y MARTÍN RM Y JAVATO MARTÍN AM. Bank card fraud in Spain, En Digital Evidence and Electronic Signature Law Review Vol. 6, pp. 67-78, p.71.

[106] Art 239.3 inciso final: A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, los mandos o instrumentos de apertura a distancia y cualquier otro instrumento tecnológico de eficacia similar.

llaves falsas a efectos de su aplicación en los delitos de robo con fuerza en las cosas.

La mayoría de las tarjetas en la actualidad son magnéticas, es decir, disponen de una banda magnética que se basa en la firma manuscrita del titular, y los números de control en el reverso de las mismas, así como en el uso de un PIN (*personal identification number*). Se trata de tarjetas fáciles de imitar, que contienen además un chip con tarjetas de memoria, incluso en ocasiones un microprocesador (*smart cards*), siendo tarjetas sin contacto con campo magnético o radiofrecuencia, que permiten la lectura a una distancia media. Este último tipo de tarjetas no encajaban dentro del artículo 239 del Código, al no funcionar mediante banda magnética. [107]

Según FARALDO CABANA[108], así como MATA Y MARTÍN Y JAVATO MARTÍN[109], la calificación que se daba a las conductas de sustracción de dinero mediante tarjetas como robo con fuerza en las cosas era discutible, ya que el artículo 237 del CP exige que la fuerza en las cosas se utilice para acceder al lugar donde se encuentran, como puede ser una caja fuerte o la habitación de un hotel. Además, es requisito esencial el empleo de fuerza para acceder al lugar donde se encuentran, lo cual en el caso del cajero no sucede ya que el dinero se expide al exterior. Las tarjetas de crédito necesitan por su parte de la introducción del número secreto, no abriéndose ninguna cerradura ni dándose acceso al espacio donde se encuentra el dinero, sino al dinero mismo, por lo que no era asimilable a la llave falsa.

Otra teoría trataba de reconducir este delito mediante uso de tarjetas, al robo con fuerza en casa habitada, edificio o local abierto al público o en

---

[107] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, pp. 52-54.

[108] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, pp. 53-63.

[109] MATA Y MARTÍN RM Y JAVATO MARTÍN AM. Bank card fraud in Spain, En Digital Evidence and Electronic Signature Law Review Vol. 6, pp. 67-78, p.72.

cualquiera de sus dependencias (artículo 241 del CP), al encontrarse el cajero en un local y realizarse el acto delictivo durante las horas de apertura del mismo, es decir, día y noche. Esta posibilidad es inconcebible para FARALDO CABANA,[110] debido a la apertura ininterrumpida del cajero, así como a la falta de concurrencia de violencia o intimidación en las personas. Además, el cajero se encuentra en todo caso en la calle, por lo que la tarjeta no era asimilable a la llave falsa.

Entre las tesis barajadas se identificó a su vez el uso de tarjetas ajenas para extraer dinero del cajero automático con el hurto**,** al no hallar el plus de desvalor que justifica la mayor penalidad del robo con fuerza en las cosas respecto al hurto.

4.3.1.2. Estafa tradicional e informática

Los pagos mediante la presentación no consentida de tarjetas ajenas en comercios para adquirir un bien o un servicio eran reconducidos por la jurisprudencia y la doctrina al tipo penal de delito de estafa tradicional regulado en el artículo 248.1 del CP.[111]

Por otro lado, el uso de tarjetas ilícitamente para llevar a cabo operaciones fraudulentas de pago ejecutadas en la red con tarjetas fue reconducido por la jurisprudencia y la doctrina al tipo delictivo de estafa informática del artículo 248.2 del CP (actual artículo 248.2 a) del CP), que fue introducido en 1995, ya que se entendía que el requisito de engaño de la estafa

[110] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, pp. 53-63.

[111] JAVATO MARTÍN A.M. Las tarjetas de crédito y débito. Aspectos penales, en Cuaderno Red de Cátedras Telefónica Nº 10, Salamanca, p. 7.

clásica solo podía darse en una relación personalista entre dos sujetos, excluyéndose la posibilidad de engañar a una máquina.[112]

Sin embargo, recurrir a la estafa informática para castigar las conductas planteaba ciertos problemas, ya que incluir el uso no autorizado de datos ajenos en la definición de manipulación informática se consideraba una vulneración del principio de legalidad por parte de la doctrina.

4.3.2. La introducción de un delito de estafa mediante tarjetas de crédito o débito, o cheques de viaje en la reforma de 2010 del CP

Para solventar los problemas de calificación penal anteriormente señalados, la LO 5/2010 introdujo en el artículo 248.2 c) del CP la infracción relativa al uso indebido de tarjetas de crédito o débito, o cheques de viaje o bien los datos obrantes en cualquiera de ellos en perjuicio de su titular o de un tercero, contemplándose la pena regulada en el artículo 249 del CP, aplicable a todas las modalidades de estafa.

La tipificación de la estafa sobre tarjetas ha producido que conductas que con anterioridad se reconducían a la estafa tradicional actualmente se localicen al tipo específico, como son el pago en un supermercado o en grandes almacenes mediante tarjeta. Lo mismo sucede con conductas que se reconducían anteriormente a la estafa informática, como el uso de tarjetas o sus datos a distancia, pagos realizados en comercio electrónico etc., los cuales pasan a subsumirse en el delito de estafa mediante tarjetas.

Sin embargo, esta nueva tipificación penal no está exenta de críticas. Entre ellas, MATA Y MARTÍN[113] considera innecesaria la modificación, ya que el uso de tarjetas o de sus datos para provocar perjuicios patrimoniales se

---

[112] JAVATO MARTÍN A.M. Las tarjetas de crédito y débito. Aspectos penales, en Cuaderno Red de Cátedras Telefónica Nº 10, Salamanca, p. 13.

[113] MATA Y MARTÍN RM. Comentarios prácticos al código penal, Navarra, p.175.

trataba en la práctica de una modalidad de estafa convencional o informática. En este sentido, continúa diciendo que la inclusión de un supuesto específico únicamente logra aportar una mayor complejidad al tratamiento penal, ya que la diversificación del delito de estafa provoca la pérdida de estructuración sistemática.[114]

4.3.3. Clases de tarjetas

El objeto material de la modalidad de estafa contemplada en el artículo 248.2 c) del CP se trata únicamente de tarjetas de crédito, de débito, o cheques de viaje. Esto supone que quedan fuera del tipo delictivo las tarjetas de compra o de cliente, de caja abierta o permanente, prepago, cibertarjetas o tarjetas virtuales etc. El delito que se cometa con estos instrumentos excluidos del tipo específico se reconducen a la estafa clásica del artículo 248.1 CP, o bien a la estafa informática si es un pago no presencial del artículo 248.2 a) del CP.[115]

4.3.3.1. Tarjetas de crédito

Las tarjetas de crédito, al igual que las tarjetas de débito, se tratan de documentos mercantiles emitidos por entidades bancarias o financieras.

---

[114] En opinión de MATA Y MARTÍN y GALÁN MUÑÓZ, habría sido de mayor interés que la reforma del CP en lugar de ampliar aún más la protección penal existente frente al efectivo uso o abuso de esta clase de instrumentos, se hubiera adaptado la regulación existente a las nuevas realidades del mercado, mediante la inclusión, por ejemplo, en el concepto de llave falsa de otras tarjetas o medios de pago no magnéticos, así como a las *Smart Cards*. MATA Y MARTÍN, RM. Y GALÁN MUÑÓZ, A. Propuestas de política legislativa sobre el robo de identidad. En Cahiers de defense sociale, Numéro Extraordinaire á l`occasion du Duoziéme Congress des Nations Unies pour la prévention du crime et la justice pénale Salvador, Brésil, 2010, pp. 57-66, p.63.

[115] JAVATO MARTÍN A.M. Las tarjetas de crédito y débito. Aspectos penales, en Cuaderno Red de Cátedras Telefónica Nº 10, Salamanca, p. 9.

En ellas se permite al titular acceder a una línea de crédito con la entidad emisora de la tarjeta. Además, las tarjetas de crédito podrán usarse bien como instrumento de pago o como vehículo mediante el que acceder a un adelanto en efectivo, sin necesidad de autorización de la entidad financiera del comprador, ni que el comprador tenga que disponer de fondos para llevar a cabo el pago, ya que la operación realizada se carga posteriormente, a diferencia de lo que ocurre en las tarjetas de débito, que se cargan inmediatamente, comprobando de manera instantánea la insuficiencia de fondos. El único límite que se prevé es el establecimiento de un gasto máximo diario o mensual, o que pueda realizarse en una sola operación.[116]

La apariencia física de las tarjetas de crédito es idéntica a la que presentan las tarjetas de débito, caracterizándose por tratarse de un soporte de plástico que posee una banda magnética en la que se encuentran codificados los datos del titular. En la superficie de plástico figuran el nombre del titular, la fecha de caducidad y una secuencia de números que se corresponde con el sistema de identificación preestablecido para los sistemas de pago.

A mayores, se encuentran presentes una serie de elementos que tratan de garantizar la seguridad de la tarjeta, como son hologramas, la firma del titular de la misma y el código con el que se valida la tarjeta a la hora de llevar a cabo compras a distancia, el cual se compone de tres cifras y se encuentra impreso en el reverso de la tarjeta.

Cabe señalar que recientemente se ha venido incluyendo en las tarjetas de crédito un chip de seguridad que trata de evitar la práctica conocida como *skimming*. Sin embargo, esto no evita que esta clase de tarjetas puedan sufrir

---

[116] JAVATO MARTÍN A.M., La falsificación de las tarjetas de crédito y débito. Análisis del artículo 399 bis del Código Penal, en La Ley penal, No 101, Sección Estudios, Valladolid, p.3.

el borrado de algunos datos por medio de la variación del voltaje, o que el delincuente proceda a cortar el chip para extraerlo de la tarjeta. [117]

Entre las clases de tarjetas de crédito, encontramos, en primer lugar, aquellas que son emitidas y gestionadas por entidades bancarias o asociaciones de las mismas, haciendo uso de un contrato de franquicia con algunas de las compañías de tarjetas de crédito como pueden ser Mastercard o Visa, entre otras. Este sistema es de carácter cuatripartito, de modo que los sujetos intervinientes en la relación son un comprador que utiliza la tarjeta de crédito como medio de pago, una entidad de crédito que expide la misma, el empresario que es pagado con la tarjeta por la venta efectuada y finalmente la entidad de crédito que cobra en favor del empresario.

En segundo lugar, encontramos las denominadas *Travel and Entretainment Cards(T&E)*, que son aquellas emitidas por empresas que vinculan su admisión con establecimientos que ofrecen bienes y servicios, es decir, son tarjetas que sirven para llevar a cabo el pago de las compras que realicen los titulares o bien realizar el suministro de efectivo de la entidad bancaria. En este caso, el sistema de pago es tripartito cerrado, lo que supone que la propietaria de la marca de la tarjeta se ocupa a su vez de su emisión y gestión. Algunas de estas tarjetas de crédito son las American Express, Diners Club o bien JCB.[118]

---

[117] JAVATO MARTÍN A.M., La falsificación de las tarjetas de crédito y débito. Análisis del artículo 399 bis del Código Penal, En La Ley penal, No 101, Sección Estudios, Valladolid, 2013, pp. 3-5.

[118] JAVATO MARTÍN A.M., La falsificación de las tarjetas de crédito y débito. Análisis del artículo 399 bis del Código Penal, En La Ley penal, No 101, Sección Estudios, Valladolid, pp. 3 y 4.

4.3.3.2. Tarjetas de débito

Las tarjetas de débito se diferencian de las tarjetas de crédito en la inexistencia de relación crediticia entre la entidad financiera y su titular, lo que supone que el sujeto únicamente podrá realizar los pagos y obtener dinero en efectivo cuando haya sido previamente depositado por el titular en una entidad bancaria.

Actualmente, existen supuestos de tarjetas mixtas que operan hasta determinada cantidad como tarjetas de débito, y una vez alcanzada esa cifra, como tarjetas de crédito, como son la tarjeta Mixta Visa Clásica Halifax o la tarjeta Díez de BBVA.[119]

4.3.3.3. Cheques de viaje

Los cheques de viaje se tratan de títulos valores librados por las instituciones bancarias, financieras o grandes compañías turísticas a nombre de la persona que firma su emisión. Al igual que las tarjetas de crédito y débito, se tratan de documentos mercantiles cuya finalidad es facilitar a los viajeros la disponibilidad de su dinero en aquellos viajes que realicen al extranjero, evitando los riesgos que se derivan del traslado de dinero en efectivo.[120]

4.3.3.4. Otras modalidades de tarjetas

Aparte de las clases de tarjetas ya mencionadas, existen otras que no entran dentro del ámbito de aplicación de la estafa mediante tarjetas bancarias del artículo 248.c) del CP, sobre las cuales haremos una breve referencia.

---

[119] JAVATO MARTÍN A.M., La falsificación de las tarjetas de crédito y débito. Análisis del artículo 399 bis del Código Penal, En La Ley penal, No 101, Sección Estudios, Valladolid, p 4.

[120] JAVATO MARTÍN A.M., La falsificación de las tarjetas de crédito y débito. Análisis del artículo 399 bis del Código Penal, En La Ley penal, No 101, Sección Estudios, Valladolid, p 6 y 7.

Entre las tarjetas que quedan por mencionar, destacan entre otras las tarjetas prepago, que son aquellas en las que el bien o servicio se abona con anterioridad a su utilización, reclamando posteriormente la entrega del bien o la prestación de servicios por medio de la información grabada en el chip o la banda magnética. Serían tarjetas prepago las tarjetas de transporte público y las tarjetas regalo que se ofrecen en los grandes almacenes, entre otras. La diferencia fundamental con las tarjetas de débito y crédito es que en estas la compra se realiza de manera online, existiendo una conexión directa entre el comerciante que recibe la tarjeta para pagar y la entidad emisora, mientras que en las tarjetas prepago se lleva a cabo de manera offline.

Otras tarjetas a destacar serían las cibertarjetas o tarjetas virtuales, utilizadas mayormente para pagos por Internet debido a su alto nivel de seguridad; las tarjetas de compra, comerciales, de cliente o privativas, que ofrecen los comerciantes o agrupaciones de los mismos otorgando unas condiciones determinadas y favorables en las compras realizadas en sus establecimientos, pero sin otorgar ningún crédito ni pudiéndose obtener dinero en efectivo a través de ella (Ej. Tarjeta de compra el Corte Inglés); y finalmente las tarjetas de caja abierta o permanente, que son aquellas tarjetas bilaterales que permiten únicamente obtener fondos y realizar operaciones bancarias por medio de las redes de cajeros automáticos de una determinada entidad bancaria, existiendo previamente una cuenta o depósito asociado a la tarjeta.[121]

[121] JAVATO MARTÍN A.M., La falsificación de las tarjetas de crédito y débito. Análisis del artículo 399 bis del Código Penal, En La Ley penal, No 101, Sección Estudios, Valladolid, pp.4-6.

5. CONCURSOS DE DELITOS

5.1. ESTAFA INFORMÁTICA

5.1.1. Daños informáticos

Se encuentran regulados en el artículo 264.2 del CP, castigando a aquel que destruya, altere, inutilice o dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

La doctrina tiende a presentarlo como uno de los delitos más frecuentes y graves dentro del ámbito informático, provocando en un 8% de supuestos la paralización de la actividad durante al menos un día, sumado a las pérdidas económicas.[122]

La estafa informática del artículo 248.2 a) del CP podrá entrar en relación de concurso con el delito de daños informáticos cuando el defraudador a la hora de llevar a cabo la manipulación informática o artificio semejante, provoque el borrado de datos del sistema informático atacado, o incluso la interrupción del sistema. El concurso será real, puesto que afecta cada una de las conductas a bienes jurídicos diferentes, debiendo cada una de ellas castigarse de modo independiente, aunque esto únicamente sucederá cuando los daños informáticos causados para la perpetuación de la estafa sean más de los imprescindibles para la comisión de la estafa, ya que en caso contrario podría valorarse como responsabilidad civil, pero no de manera penal.[123]

5.1.2. Falsedad documental

A su vez, la manipulación informática llevada a cabo en la estafa informática podrá entrar en concurso ideal de delitos con la falsedad

---

[122] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, p. 137.

[123]DEVIA GONZÁLEZ, EA. Delito informático: Estafa Informática del artículo 248.2 del Código Penal, Universidad de Sevilla, pp. 327 y 328.

documental del Capítulo II del CP, puesto que el artículo 26 del CP considera documento cualquier soporte material que incorpore datos, hechos o narraciones con eficacia probatoria o de cualquier otro tipo y que tengan relevancia jurídica.[124]

5.2. ESTAFA CON TARJETAS BANCARIAS

5.2.1. Falsedad en documento mercantil

En el ámbito de las estafas con tarjetas bancarias en el pago tanto tradicional como electrónico encontramos un concurso medial de delitos[125] con la falsedad en documento mercantil,[126] si una vez se paga con la tarjeta ajena se simula la firma del titular legítimo de la misma en el ticket de compra expedido por el aparato lector de la tarjeta. En relación al hurto previo de la tarjeta, cabe señalar que se absorbe en las estafas.

En el caso de que exista coautoría en esta actuación, es decir, si varias personas estafan en una tienda con tarjetas ajenas, va a ser irrelevante quien ha firmado los tickets de compra, ya que todos son autores de la falsedad, al no

---

[124] GARCÍA SERVIGÓN, J. El fraude informático en España e Italia. Tratamiento jurídico penal y criminológico. En Revista cuatrimestral de las facultades de derecho y ciencias económicas y empresariales, nº 74, p. 295.

[125] Artículo 77 CP: .1Lo dispuesto en los dos artículos anteriores no es aplicable en el caso de que un solo hecho constituya dos o más delitos, o cuando uno de ellos sea medio necesario para cometer el otro. .3 En el segundo, se impondrá una pena superior a la que habría correspondido, en el caso concreto, por la infracción más grave, y que no podrá exceder de la suma de las penas concretas que hubieran sido impuestas separadamente por cada uno de los delitos. Dentro de estos límites, el juez o tribunal individualizará la pena conforme a los criterios expresados en el artículo 66. En todo caso, la pena impuesta no podrá exceder del límite de duración previsto en el artículo anterior.

[126] Artículo 392 CP: El particular que cometiere en documento público, oficial o mercantil, alguna de las falsedades descritas en los tres primeros números del apartado 1 del artículo 390, será castigado con las penas de prisión de seis meses a tres años y multa de seis a doce meses.

tratarse de un delito de propia mano. El delito se imputa por tanto a todos aquellos a los que beneficia el hecho en cuestión, siempre y cuando haya sido decidido conjuntamente.[127]

No existirá falsedad en documento mercantil si al comerciante le consta que aquel que realiza la imitación de la firma no es el titular de la tarjeta, puesto que es necesario que la falsedad sea penalmente relevante, provocando una lesión o haciendo peligrar el bien jurídico protegido.[128]

5.2.2. Falsificación de tarjetas de crédito, débito o cheques de viaje

Si la estafa la lleva a cabo el autor fabricando él mismo una nueva tarjeta, existe un concurso medial de delitos[129] entre la falsificación de tarjetas de crédito y débito y cheques de viaje[130] y la estafa mediante tarjetas bancarias.

---

[127] JAVATO MARTÍN A.M. Las tarjetas de crédito y débito. Aspectos penales En Cuaderno Red de Cátedras Telefónica NO 10, Salamanca pp. 9 y 10.

[128] FARALDO CABANA P., Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Valencia, p. 76.

[129] JAVATO MARTÍN A.M., La falsificación de las tarjetas de crédito y débito. Análisis del artículo 399 bis del Código Penal, En La Ley penal, No 101, Sección Estudios, Valladolid, pp.2 y 10.

[130] Artículo 399 bis CP: El que altere, copie, reproduzca o de cualquier otro modo falsifique tarjetas de crédito o débito o cheques de viaje, será castigado con la pena de prisión de cuatro a ocho años. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o cuando los hechos se cometan en el marco de una organización criminal dedicada a estas actividades.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los anteriores delitos, se le impondrá la pena de multa de dos a cinco años.

Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

2. La tenencia de tarjetas de crédito o débito o cheques de viaje falsificados destinados a la distribución o tráfico será castigada con la pena señalada a la falsificación.

El tratamiento dado a la falsificación y alteración de tarjetas ha ido cambiando a lo largo del tiempo hasta la reforma operada por la LO 5/2010. En el Código Penal de 1973 las tarjetas bancarias eran calificadas como mercantiles, de modo que la creación de una tarjeta clonada o la manipulación de tarjetas legítimas se subsumía dentro de los artículos dedicados a este tipo de falsedades. Esta clasificación fue puesta en duda puesto que la banda magnética de la tarjeta era un elemento difícilmente incorporable al concepto de documento, problema resuelto con el Código Penal de 1995, que establecía un concepto amplio de documento en el artículo 26, que cubría las bandas magnéticas en las tarjetas.

En una segunda corriente jurisprudencial se vino reconduciendo la falsificación de tarjetas al delito de falsificación de moneda del artículo 386 del CP, debido a la interpretación realizada del artículo 387 del CP incluyendo las tarjetas de crédito y débito como dinero, así como la argumentación del TS[131] señalando que las tarjetas de crédito y débito se trataban de "dinero de plástico", de modo que la incorporación de una banda magnética en estos instrumentos de pago suponía un proceso de elaboración o fabricación tipificado por el delito de falsificación de moneda. [132]

Cabe por último hacer referencia a la problemática suscitada tras la reforma del CP operada por la LO 5/2010, en la aplicación del artículo 399 bis.3 y el artículo 248.2c) del CP. El primero hace referencia al uso de tarjeta de crédito o débito o cheque de viaje falsificado, por parte de quien no ha intervenido en su falsificación, a sabiendas de la falsedad y en perjuicio de otro.

---

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.

[131] Acuerdo del Pleno no jurisdiccional de la Sala Segunda TS de la reunión de 28-06-2002, STS de 9 de mayo de 2007.

[132] MATA Y MARTÍN RM Y JAVATO MARTÍN AM. Bank card fraud in Spain, En Digital Evidence and Electronic Signature Law Review Vol. 6, pp. 67-78, p. 73.

En este sentido, JAVATO MARTÍN[133] señala que debe de ser de aplicación el principio de alternatividad del concurso de leyes del artículo 8.4 del CP[134], de modo que la falsedad del art 399 bis 3 del CP es de aplicación preferente frente a la estafa del artículo 248.2 c) del CP, ya que tiene pena superior, prisión de 2 a 5 años, mientras que la última tiene una pena de prisión de 6 meses a 3 años. Este criterio se invierte si se aprecian circunstancias agravantes de la estafa, aumentando la pena a prisión de uno a seis años y multa de seis a doce meses. Encontramos posturas contrarias a esta, como es la expuesta en la Sentencia de la Audiencia Nacional (SAN) de 25-6-2012 que estima que la estafa quedaría absorbida en la falsedad (8.3 CP).

6. CONCLUSIONES

Primera. - El delito de estafa informática se encuentra regulado en el artículo 248.2 a) del CP. Se introdujo en el CP de 1995 para regular aquellos delitos que, si bien se asemejaban en algunos aspectos a la estafa tradicional, no terminaban de encajar con todos sus elementos, los cuales son el engaño, el error, el acto de disposición patrimonial por el sujeto activo, el perjuicio en la víctima, el ánimo de lucro y el nexo causal entre todos los requisitos.

En este sentido, la principal diferencia con la estafa tradicional se encuentra ligada con la necesidad de que la estafa informática se lleve a cabo

---

[133] JAVATO MARTÍN A.M. Las tarjetas de crédito y débito. Aspectos penales En Cuaderno Red de Cátedras Telefónica NO 10, Salamanca p. 27.

[134] Artículo 8 CP: Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de este Código, y no comprendidos en los artículos 73 a 77, se castigarán observando las siguientes reglas: 1.ª El precepto especial se aplicará con preferencia al general. 2.ª El precepto subsidiario se aplicará sólo en defecto del principal, ya se declare expresamente dicha subsidiariedad, ya sea ésta tácitamente deducible. 3.ª El precepto penal más amplio o complejo absorberá a los que castiguen las infracciones consumidas en aquél. 4.ª En defecto de los criterios anteriores, el precepto penal más grave excluirá los que castiguen el hecho con pena menor.

por medio de una manipulación informática o un artificio semejante. La introducción de este elemento supone la exclusión o la presencia indirecta del requisito de la producción de un engaño por el estafador, así como la necesidad de que exista error en la víctima. Esto es debido a que el sujeto al que va dirigida esta clase de estafa no puede ser inducido a error o a engaño, puesto que la acción fraudulenta se lleva a cabo frente a un ordenador o a una máquina, que no pueden ser engañadas ni inducidas a error, puesto que no disponen de la capacidad intelectual para pensar y decidir, propia de los seres humanos.

A su vez, cabe señalar otros elementos diferenciadores respecto a la estafa tradicional, como es la necesidad de que se produzca una transferencia no consentida de activos patrimoniales, que se trata del equivalente al acto de disposición presente en la estafa tradicional, que únicamente puede llevarse a cabo por una persona física. Este elemento transforma el sentido con el que se entiende el ánimo de lucro, de modo que no se trata de la intención de obtener un beneficio económico para sí o para un tercero, sino que se trata del ánimo de provocar una transferencia de activos patrimoniales ajenos por medio de una manipulación informática, a la cual se encuentra ligada la obtención del beneficio económico.

Segunda. – El bien jurídico protegido por un tipo penal se trata de un elemento crucial para lograr tener conocimiento de su naturaleza, extensión, límites y alcance de la protección que ofrece. Si bien la doctrina ha agrupado los nuevos tipos penales que sancionan conductas que atentan contra una variedad de bienes jurídicos haciendo uso de medios informáticos, tecnologías telemáticas e Internet dentro del concepto de delitos informáticos, se aprecia una carencia de un bien jurídico protegido propio, lo que resulta en que el bien jurídico protegido por la estafa informática sea el patrimonio.

La mayor amplitud del uso de sistemas informáticos para toda clase de tareas ha producido un incremento del alcance del ciberespacio, haciendo conveniente la especificación de bienes jurídicos propios atribuibles a los

sistemas informáticos, que aporten una mayor concreción de estos tipos penales, así como una mayor seguridad jurídica.

Concretamente, sería interesante el desarrollo de un bien jurídico colectivo. Al igual que ocurre en los delitos medioambientales, en los cuales el bien jurídico protegido es el medio ambiente, en los delitos informáticos el bien jurídico podría abarcar el correcto funcionamiento de los sistemas informáticos, al ser un elemento de gran trascendencia para el correcto funcionamiento de la sociedad y la economía nacional e internacional.

Tercera. - La estafa cometida por medio de tarjetas de crédito, débito y cheques de viaje, se trata de un tipo delictivo que se encuentra regulado en el artículo 248.2 c) del CP, que se introdujo tras la reforma operada por la LO 5/2010.

El amplio elenco de actuaciones ilícitas que pueden llevarse a cabo mediante el uso de tarjetas bancarias, que abarcan desde la adquisición ilegítima de bienes o servicios en terminales de punto de venta presenciales, hasta la realización de pagos no consentidos por medio de redes informáticas de manera no presencial y la extracción ilegítima de dinero en cajeros automáticos, ha llevado a la doctrina y a la jurisprudencia a incluir esta clase de delitos dentro de diversos tipos penales existentes con anterioridad a la reforma operada en el año 2010. En este sentido, estas conductas han sido incorporadas dentro de los tipos delictivos de hurto (art. 234 CP) y robo con fuerza sobre las cosas (art. 238 CP), estafa tradicional (art. 248.1 CP) y estafa informática (antiguo art. 248.2CP).

Las soluciones aportadas a esta clase de conductas llevadas a cabo por medio de tarjetas de crédito, débito o cheques de viaje no se consideraban satisfactorias. Respecto a la calificación de estas actuaciones como robo con fuerza en las cosas, se concluyó que no podían considerarse estas tarjetas como llaves falsas conforme al artículo 230 del CP, puesto que poseían una banda magnética, ni tampoco podía calificarse de fuerza en las cosas el acceso a un cajero automático. A su vez, se dudaba de la calificación que se le daba

como estafa informática, puesto que algunos autores entendían que se vulneraba el principio de legalidad al introducir el uso no autorizado de datos dentro de la definición de manipulación informática.

Cabe concluir que, si bien la decisión del legislador de introducir un tipo penal independiente relacionado con las tarjetas de crédito, débito y cheques de viaje soluciona los problemas interpretativos anteriormente señalados, puede dar lugar a una mayor complejidad en la estructura de la estafa.

Cuarta. - La modalidad de estafa mediante el uso de tarjetas bancarias regulada en el artículo 248.2 c) del CP es de aplicación exclusiva a las tarjetas de crédito, de débito y los cheques de viaje, lo que supone que el resto de tarjetas de pago, como pueden ser las tarjetas de compra o de cliente, las tarjetas de caja abierta o permanente, las tarjetas prepago y las cibertarjetas entre otras quedan excluidas de este tipo penal. Los fraudes que se cometan haciendo uso de estos medios de pago se reconducirán a la estafa clásica, o bien a la estafa informática en caso de que el pago realizado sea no presencial.

Quinta. - Se ha producido un incremento significativo de la cantidad de delitos informáticos a nivel nacional en la última década, tal y como muestran las estadísticas del Observatorio Español de Delitos Informáticos expuestas al comienzo del trabajo. Esta cifra será mucho mayor, bajo mi punto de vista, al término del presente año, debido al aumento del uso de Internet, así como el incremento del teletrabajo como consecuencia de la pandemia Covid-19.

Sexta. - El aumento de esta clase de delitos a nivel tanto nacional como internacional, así como los efectos producidos por la globalización han provocado que las actuaciones tomadas al respecto a nivel transnacional cobren en la actualidad una relevancia mayor.

Es por ello, que es de vital importancia que se continúen realizando esfuerzos normativos a nivel internacional para afianzar la cooperación interestatal. Con este objetivo, se redactó el Convenio de Budapest de 23 de

noviembre de 2001 en el ámbito del Consejo de Europa, que trató de armonizar los elementos del Derecho penal de los Estados Miembros que tuvieran relación con conductas ilícitas por medios informáticos, así como la Directiva 2013/40/UE del Parlamento Europeo y del Consejo y la Directiva 2019/13 del Parlamento Europeo y del Consejo que tratan de armonizar las penas y tipos penales de esta clase de delitos a nivel de la UE.

7. BIBLIOGRAFÍA Y MATERIALES DE REFERENCIA

7.1. BIBLIOGRAFÍA

ANTÓN ONCECA, José. Estafa, en Nueva Enciclopedia jurídica, Tomo IX (dir. MASCAREÑAS Carlos-E), Ed. Franciso Seix SA, pp. 69 y ss., Barcelona, 1958.

ARÁNGUEZ SÁNHEZ, Carlos. La falsificación de moneda, Editorial Bosch, Barcelona, 2000.

AZCONA ALBARRÁN Carlos David. Tarjetas de pago y derecho penal. Un modelo interpretativo del art. 248.2 c), Barcelona, 2012.

BAJO FERNÁNDEZ, Miguel. Los delitos de estafa en el Código Penal, Editorial Universitaria Ramón Arces, Madrid, 2004.

BALMACEDA HOYOS, Gustavo. El delito de estafa informática en el derecho europeo continental, en Revista de derecho y ciencias penales nº 17, pp. 111-149, San Sebastián(Chile), 2011.

CÁCERES RUIZ, Luis. Delitos contra el patrimonio: aspectos penales y criminológicos. Especial referencia a Badajoz, Editorial Vision Net, Madrid, 2006.

CHOCLÁN MONTALVO, José Antonio. El delito de estafa. Nº 2, Editorial Bosch, Barcelona, 2009.

CORCOY BIDASOLO, Mirentxu. Problemática de la persecución penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos, en Eguzkilore: Cuaderno del Instituto Vasco de Criminología, nº 21,2007, pp. 7-32.

DE LA CUESTA ARZAMENDI, José Luis. Derecho penal informático, Editorial Thomsons Reuters, Navarra, 2010.

DEVIA GONZÁLEZ, Edmundo Ariel. Delito informático: Estafa Informática del artículo 248.2 del Código Penal (dir. POLAINO NAVARRETE Miguel), Universidad de Sevilla, 2017.

FARALDO CABANA, Patricia. Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico, Editorial Tirant lo Blanch, Valencia, 2009.

FERNÁNDEZ MORÓN, Alba. Aspectos esenciales del delito de estafa en el Código Penal español (dir. PÉREZ SAUQUILLO MUÑOZ Carmen), Universidad de Alcalá, 2019.

FERNÁNDEZ ROZAS, José Carlos. Nuevas disposiciones de la Unión Europea sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo – El Blog de José Carlos Fernández Rozas. Disponible en https://fernandezrozas.com/2019/05/15/nuevas-disposiciones-de-la-union-europea-sobre-la-lucha-contra-el-fraude-y-la-falsificacion-de-medios-de-pago-distintos-del-efectivo/ (consulta 23/05/2020).

FERNÁNDEZ TERUELO, Javier Gustavo, Respuesta penal frente a fraudes cometidos en Internet: Estafa, estafa informática y los nudos en la red, en Revista de derecho penal y criminología 2.a Época, nº 19, pp. 217-243. 2007.

GARCÍA GARCÍA, Diego Eloy, El phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (REC. 1402/2016), en Rev. Boliv. de Derecho nº 25, pp. 650-659, 2018.

GARCÍA GARCÍA-CERVIGÓN, Josefina. El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico, en Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales nº 74, pp. 289-308, 2008.

GALÁN MUÑOZ, Alfonso. El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 CP, Editorial Tirant lo Blanch, Valencia, 2005.

GARCÍA NOGUERA, Isabel. La STJCE de 13 de septiembre de 2005, Ed. Aranzadi, 2007.

GARCÍA NOGUERA, Isabel. La reforma penal de la falsificación, tráfico y uso ilícito de tarjetas bancarias en Revista de Internet, Derecho y Política, Universitat Oberta de Catalunya, 2007.

GARCÍA SERVIGÓN, Josefina. El fraude informático en España e Italia. Tratamiento jurídico penal y criminológicos. En Revista cuatrimestral de las facultades de derecho y ciencias económicas y empresariales, nº 74, España, 2008.

HERRERA MORENO, Miriam. El fraude informático en el derecho penal español. En Revista de Actualidad Penal, nº 39, Sevilla, 2001 pp. 954 y ss.

JAVATO MARTÍN, Antonio María. La falsificación de las tarjetas de crédito y débito. Análisis del artículo 399 bis del Código Penal, en La Ley penal, nº 101, Sección Estudios, Ed. La Ley, Valladolid, 2013.

JAVATO MARTÍN, Antonio María, Las tarjetas de crédito y débito. Aspectos penales, en Cuaderno Red de Cátedras Telefónica, nº 10, Salamanca, 2013.

JIMÉNEZ GARCÍA, Joaquín. Delito e informática: Algunos Aspectos De Derecho Penal Material, en Revista del Instituto Vasco de Criminología, San Sebastián, nº20, pp. 198-215, 2006.

MATA Y MARTÍN, Ricardo M. De las estafas, en Comentarios prácticos al Código Penal (dir. GÓMEZ TOMILLO Manuel), Editorial Aranzadi, pp. 165 y ss., Pamplona, 2015.

MATA Y MARTÍN, Ricardo M. Delincuencia informática y Derecho penal, Editorial Edisofer, Madrid, 2001.

MATA Y MARTÍN, Ricardo M. Y GALÁN MUÓZ, Alfonso. Propuestas de política legislativa sobre el robo de identidad. En Cahiers de defense sociale, Numéro Extraordinaire á l`occasion du Duoziéme Congress des Nations Unies pour la prévention du crime et la justice pénale Salvador, Brésil, 2010, pp. 57-66.

MATA Y MARTÍN Ricardo M Y JAVATO MARTÍN Antonio María. Bank card fraud in Spain, En Digital Evidence and Electronic Signature Law Review, Vol. 6, pp. 67-78, 2009.

PALOMINO MARTIN, Jose María. Derecho penal y nuevas tecnologías. Hacia un sistema informático para la aplicación del derecho penal, Editorial Tirant lo Blanch, Valencia., 2006.

PÉREZ LUÑO Antonio Enrique. Manual de Informática y Derecho, Editorial Ariel, Barcelona, 1996.

PÉREZ MACHÍO, Ana Isabel. Dos problemas particulares de cara a la persecución de los delitos informáticos, en Derecho penal informático (dir. DE LA CUESTA ARZAMENDI José Luis/ coord. DE LA MATA BARRANCO Norberto Javier), Editorial Thomsons Reuters, pp. 247-277, 2010.

PÉREZ MANZANO, Mercedes. Acerca de la Imputación Objetiva de la Estafa, en hacia un Derecho Penal Económico Europeo, Universidad Autónoma de Madrid, pp. 285-309, Madrid, 1995.

PÉREZ MANZANO, Mercedes. Las defraudaciones (I). Las estafas, en Comprendido de Derecho Penal Parte Especial Volumen II (dir. BAJO FERNÁNDEZ Miguel), pp. 447 y ss., Madrid, 1998.

RAMÍREZ BEJERANO, Egil Emilio Y AGUILERA RODRÍGUEZ, Ana Rosa. Los delitos informáticos. Tratamiento Internacional, Disponible en: http://www.eumed.net/rev/cccss/04/rbar2.htm (consulta 20/04/2020).

ROMEO CASABONA, Carlos María. Delitos informáticos de carácter patrimonial, en Revista iberoamericana de derecho informático, nº 9-11, pp. 413-442, 1996.

ROMEO CASABONA, Carlos María. Poder informático y seguridad jurídica, Editorial Fundesco, Madrid, 1988.

SÁNCHEZ BERNAL, Javier. El bien jurídico protegido en el delito de estafa informática, en Cuadernos de Tomás nº 1, pp. 105-121, 2009.

SILVIA SÁNCHEZ, Jesús María. El nuevo Código Penal. Comentarios a la reforma, Editorial La Ley, Madrid, 2012.

VILLACAMPA ESTIARTE, Carolina. 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?, en Diario La Ley, n.º 6994, 2008.

7.2 MATERIALES DE REFERENCIA

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Pena.

Ley 16/2009, de servicios de pago.

Informe CONCRIME 1998.

Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

Directiva de la UE 2019/713 del Parlamento Europeo y del Consejo de 17 de abril de 2019, relativa la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.

Código Penal Alemán del 15 de mayo de 1871, con la última reforma del 31 de enero de 1998.

Código Penal italiano, con la reforma de la Ley Nº 547 de 23/12/1993.

Informe OCDE 1986 Delitos de informática: análisis de la normativa jurídica.

Directrices de la OCDE para la seguridad de sistemas y redes de información 1992.

Resolución ONU 45/121, de 14 de diciembre de 1990.

Manual de las Naciones Unidas para la Prevención y Control de Delitos informáticos de 1994.

Convenio Europeo sobre Delincuencia Informática de Budapest de 20 de noviembre de 2001, sobre política penal común.

ESTADISTICAS - OEDI | Observatorio Español Delitos Informáticos. Disponible en: https://oedi.es/estadisticas/ (consulta 14/05/2020).

Página oficial de la DGP-Comisaría General de Policía Judicial. Disponible en: https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html (consulta 14/05/2020).

GDT - Grupo de Delitos Telemáticos. Disponible en: https://www.gdt.guardiacivil.es/webgdt/faq.php(consulta 14/05/2020).

Qué es INCIBE | INCIBE. Disponible en: https://www.incibe.es/que-es-incibe(consulta 14/05/2020).

Europa se refuerza penalmente frente a los ataques a los sistemas de Información | ECIJA. Disponible en: https://ecija.com/sala-de-prensa/europa-se-refuerza-penalmente-frente-a-los-ataques-a-los-sistemas-de-informacion/(consulta 29/05/2020).