EL DELITO DE ESTAFA INFORMÁTICA EN EL DERECHO EUROPEO CONTINENTAL

THE COMPUTER FRAUD IN THE EUROPEAN CONTINENTAL LAW

GUSTAVO BALMACEDA HOYOS *
Universidad de Los Andes
Chile

RESUMEN

En Chile el delito de "estafa informática" no se encuentra específicamente "legislado". Por ello, resulta relevante tener a la vista los diferentes sistemas de la estafa informática del Derecho europeo continental a la hora de tomar una decisión legislativa. A esto se dedica el presente trabajo.

Palabras clave: *estafa, engaño, estafa informática.*

ABSTRACT

In Chile the crime of "computer fraud" it is not "legislated specifically". For this reason, at the time of making a legislative decision turns out relevant to study the different computer fraud´s systems from the European continental Law. To this goal the present work is about.

Key words: *swindle crime, deceit, computer fraud.*

* Abogado. Doctor en Derecho Penal por la Universidad de Salamanca, España. Profesor de Derecho Penal y Derecho Procesal Penal de Universidad de los Andes, Chile. Dirección postal: San Carlos de Apoquindo 2200, Las Condes, Santiago, Chile. Correo electrónico: gbalmaceda@uandes.cl y gbalmah@gmail.com.

** Abreviaturas: art(s): artículo(s); p. ej.: por ejemplo; TS: Tribunal Supremo español; RJ: Repertorio Aranzadi de Jurisprudencia; STS: sentencia del Tribunal Supremo español.

I. INTRODUCCIÓN

En este entorno se puede hablar indistintamente de "fraude" o "defraudaciones". Desde un punto de vista objetivo, ambas figuras aluden a una conducta (*modus operandi*) que implica un montaje o artimaña; y, desde un punto de vista subjetivo, conllevan un ánimo de perjuicio ajeno en beneficio personal (*animus decipiendi*).

La voz "fraude informático", por su parte, es equivalente a "defraudaciones informáticas". Se trata, a nuestro juicio, de una categoría criminológica, funcional y amplia que concentraría una multiplicidad de comportamientos heterogéneos (contra intereses económicos difusos), beneficiados por la naturaleza de los sistemas informáticos y su forma de trabajo.

De otro lado, la voz "estafa informática" al parecer alude exclusivamente a las defraudaciones "patrimoniales" ocasionadas por medios informáticos (relación de género a especie con el "fraude informático"). Es decir, se trataría de un concepto más restringido que el de "fraude informático", y a este ilícito nos referiremos este trabajo.

La doctrina comparada mayoritaria –que aceptamos parcialmente– sostiene que el patrimonio, comprendido en sentido equivalente al delito de estafa tradicional, es el bien jurídico-penal protegido en la estafa informática[1]. No obstante (y aquí se sitúa nuestra diferencia con la opinión tradicional), nos parece que el delito de "fraude informático" (en relación de género a especie con la "estafa informática") resume una multiplicidad de conductas lesivas de múltiples intereses económicos –más allá del patrimonio individual microsocial–, realizados con ánimo de obtener una utilidad económica y explotando las singularidades de los medios informáticos y su actividad. No obstante, debería objetarse toda tesis que estime que se tienen que proteger en la estafa informática otros bienes jurídico-penales supuestamente independientes y dominantemente informáticos, como conseguirían ser la propia información contenida en dichos sistemas, o su intangibilidad[2].

En directa relación con el aspecto recién referido se encuentra la naturaleza jurídica de nuestro delito. En el Derecho europeo continental la mayoría de la doctrina estima que el delito de estafa informática debería estudiarse estrechamente vinculado al delito de estafa tradicional. Sin embargo, las opiniones se dividen a la hora de determinar los "límites" de esa proximidad[3]:

i) En Alemania, la mayoría de la doctrina utiliza como criterio restrictivo para la aplicación del delito de estafa informática, señalando que el comportamiento debe corresponderse a un "engaño" hacia personas como en la estafa. Esto trae como

[1] Sobre esto, con múltiples referencias, BALMACEDA HOYOS, Gustavo, *El delito de estafa informática*, Santiago, Ediciones Jurídicas de Santiago, 2009, pp. 115 y ss., 129 y ss.

[2] Sobre este tema ya nos hemos referido en otro lugar, confróntese BALMACEDA HOYOS, Gustavo, *op. cit.*, pp. 138 y ss.

[3] Con múltiples referencias, BALMACEDA HOYOS, Gustavo, *op. cit.*, pp. 115 y ss.

consecuencia que sólo existiría una influencia sobre un proceso de tratamiento de datos cuando difiera el resultado que se habría obtenido con un proceso adecuado; que únicamente se tendrían en cuenta tales procesos cuando sean relevantes para el patrimonio; que el perjuicio patrimonial tendría que ser consecuencia directa de la disposición patrimonial; que no se requeriría que el operador del sistema y el perjudicado sean idénticos; y, que se trataría de un delito defraudatorio, no de "apropiación".

ii) En Italia, por su parte, la mayoría de la doctrina sostiene que el delito de estafa informática se inspira en el esquema de la estafa tradicional, aplicándose la estafa informática a aquellos casos en que el computador reemplazaría el proceso decisional del ser humano.

iii) Por último, en España, se sostiene que el delito de estafa informática presenta una estrecha vecindad con el delito de estafa clásico, emanándose dicha conexión, tanto del propio fin de cierre de lagunas alcanzado por el legislador con la tipificación de este delito, como de su propia proximidad sistemática. Con la base expuesta, en España algunos interpretan a la estafa informática como una "estafa impropia", o como una "estafa general", pero con rasgos que obstaculizan su equiparación total.

En nuestra opinión, debería efectuarse una lectura alternativa del tipo de estafa clásico con el objeto de viabilizar la inclusión en su seno de los comportamientos que se contemplan en la estafa informática[4]. Así, su expresa tipificación solamente representaría una interpretación auténtica de los límites del delito de estafa tradicional. A las conclusiones anteriores hemos llegado a través del siguiente razonamiento:

i) Las máquinas se programan y ejecutan las órdenes que se le den, por lo que nunca se engañaría a una máquina[5];

ii) El error no sería un elemento autónomo del delito de estafa (sobre todo en aquellos países –como es el caso de Chile– donde el legislador no otorga una definición general del delito de estafa tradicional, limitándose a manifestar una serie de extraños y anticuados ejemplos) [6]; y,

iii) El dominio de la disposición no correspondería al computador, pues únicamente materializa las órdenes para las que fue programado, sino al que prepara los equipos involucrados, que siempre será un ser humano[7].

[4] BALMACEDA HOYOS, Gustavo, *op. cit.*, pp. 355 y ss.
[5] BALMACEDA HOYOS, Gustavo, *op. cit.*, pp. 171 y ss.
[6] BALMACEDA HOYOS, Gustavo, *op. cit.*, pp. 220 y ss.
[7] BALMACEDA HOYOS, Gustavo, *op. cit.*, pp. 223 y ss.

Teniendo presente lo anterior, ¿sería entonces necesaria una prisa por parte del legislador chileno, en orden a que tipifique específicamente al delito de "estafa informática"? Conforme a lo que hemos expuesto, consideramos que no. No obstante, quizá sería conveniente que lo haga, para otorgar seguridad jurídica. De esta manera, como ya se adelantó, nos parece que su tipificación constituiría una interpretación auténtica de lo que siempre fue una estafa.

Así las cosas, resulta forzoso echar un vistazo a la regulación legal de la estafa informática en el Derecho comparado, en especial, en aquellos países que siempre han servido de referente para el Derecho chileno y sudamericano en general, esto es, en Alemania, Italia, y España. Esto, con el propósito de dar pistas al legislador chileno a la hora de tomar una decisión legislativa[8].

A esta altura se hace necesario hacer presente que en Chile existe un proyecto de ley sobre este tema, contenido en el Boletín 3083-07 de 2/10/2002. Nos parece que ha transcurrido un tiempo más que razonable para que dicho proyecto se haya transformado en ley. No obstante, ello no ha acaecido. Hasta el cierre de esta investigación su tramitación seguía congelada en el segundo trámite constitucional. Por lo anterior, no nos dedicaremos a analizar el referido proyecto. Lo haremos en el futuro, cuando se vea con mayor certeza su camino a "ser ley".

II. UNA APROXIMACIÓN A LOS DIFERENTES SISTEMAS LEGISLATIVOS DE LA ESTAFA INFORMÁTICA EN EL DERECHO EUROPEO CONTINENTAL

En *Alemania* la *estafa informática* se encuentra regulada en el § 263a[9] del Código Penal Alemán. La norma[10] fue creada por el Art. 1 Nº 9 de la 2ª Ley de lucha contra la crimi-

[8] BALMACEDA HOYOS, Gustavo, *op. cit.*, pp. 271 y ss.

[9] "§ 263a Estafa informática (1) Quien, con el propósito de obtener una ventaja patrimonial antijurídica para sí o para un tercero, perjudica el patrimonio de otro, influyendo en el resultado de un proceso de tratamiento de datos, a través de una errónea configuración del programa, a través del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos, o de otra manera a través de una intervención no autorizada en el proceso, se castiga con privación de libertad de hasta cinco años o con multa. (2) Los párrafos 2 a 7 del § 263 son aplicables según corresponda. (3) Quién prepara un delito según el párrafo 1, mientras produce un programa informático cuyo objetivo es la comisión de tal hecho, proporcionado para sí o para un tercero, lo ofrece, guarda, o se lo deja a otro, se castiga con privación de libertad de hasta tres años o con multa. (4) En los casos del párrafo 3 son aplicables, según corresponda, los párrafos 2 y 3 del § 149" (traducción del autor).

[10] i) Para el estudio de la historia fidedigna de la ley, véase TIEDEMANN, Klaus, "§ 263a", en *Leipziger Kommentar zum Strafgesetzbuch*, Berlin, De Gruyter Recht, 1997, VI, números de margen 1 y ss.; LACKNER, Karl, "Zum Stellenwert der Gesetzestechnik. Dargestellt an einem Beispiel aus dem Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität", en AAVV, *Festschrift für Herbert Tröndle*, Berlin - New York, Walter de Gruyter, 1989, p. 43 y ss. ii) Sobre su importancia práctica, KINDHÄUSER, Urs, "§ 263a", en *Nomos Kommentar zum Strafgesetzbuch*, Nomos, Baden Baden, 2005, número de margen 12; TIEDEMANN, Klaus, *§ 263a…*, número de margen 7. iii) Para las bases criminológicas, SIEBER, Ulrich, *Computerkriminalität und Strafrecht*, Köln - Berlin - Bonn - München, Carl Heymanns Verlag KG, 1980, pp. 126 y ss., TIEDEMANN, Klaus, *263a…*, número de margen 3. iv) Y, para su desarrollo fuera de Alemania, TIEDEMANN, Klaus, *263a…*, números de margen 8 y ss.

nalidad económica (*Gesetz zur Bekämpfung der Wirtschaftskriminalität*), y fue ampliada por el Art. 1 Nº 10 de la 35ª Ley de modificación del Derecho penal (*strafrechtsänderungsgesetz*) de 22/11/2003[11]. Se dice que la introducción de un delito *paralelo* al tipo de estafa consistía en una necesidad político-criminal ineludible, debido a la emergente utilización de procesamientos de datos, particularmente en la organización del servicio de pagos en el ámbito bancario, donde se había incrementado el peligro de uso abusivo, y en donde –en opinión de la mayoría[12]– los tipos penales vigentes no podían comprender tales comportamientos, porque –en su opinión–, un daño patrimonial no se originaría por la disposición condicionada del error de una persona (natural), pues ocurrido el perjuicio patrimonial por una intervención ilícita en el sistema del proceso de tratamiento de datos no se produciría un engaño en la persona encargada del control. Por otra parte, en el párrafo 3º del § 263a del Código Penal Alemán se contiene una *expansión de penalidad* de actos preparatorios. Esto se debió a una decisión marco del Consejo de la *Unión Europea* de 28/5/2001 para la lucha contra la estafa y falsificación en relación con los medios de pago ilícitos, sin que el legislador alemán quisiera marcar un propio acento que supere esto, habiendo superado, al parecer, sus compromisos legales con Europa[13].

La versión original[14] del § 263a del Código Penal Alemán se inspiraba estrechamente en el § 263[15] del mismo Código. Sin embargo, la misma, se extendió por parte del consejo de expertos del comité legal, también a los casos de uso no autorizado de datos, impulsado por la norma sobre los elementos estructurales de la estafa y también por los delitos contra la propiedad –en el sentido del hurto mediante engaño ("*Trickdiebstahls*", que coincide con el robo con fuerza del art. 440 Nº 3[16] del Código Penal chileno)–, que incluye los tipos de apropiación indebida e infidelidad[17]. Sobre esto se ha afirmado[18] que aquí se formaría, como frecuentemente ocurre en la legislación actual, perceptiblemente, la versión del tipo de una norma principalmente orientada a algunas pocas constelaciones de casos, ignorándose que la regulación comprendería casos no dignos de penalidad por causa de su formulación unívoca y también abstracta. Así, se dice que por la ampliación del "uso no autorizado de datos" la norma perdió su simetría

[11] Véase CRAMER, Peter y PERRON, Walter, "§ 263a", en SCHÖNKE Adolf, SCHRÖDER Horst y CRAMER Peter (eds.), *Strafgesetzbuch Kommentar*, München, C.H. Beck, 2006, número de margen 1.

[12] Sobre esto, TIEDEMANN, Klaus, *263a…*, número de margen 2; ZAHN, Gesche, *Die Betrugsähnlichkeit des Computerbetrugs (§ 263a StGB)*, Aechen, Shaker Verlag, 2000, pp. 21 y ss.

[13] Véase CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 1.

[14] Así, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 2.

[15] Esta norma, en cuanto a lo que nos interesa, dice: "Quién, con el fin de obtener una ventaja patrimonial ilícita para sí o a un tercero, perjudique el patrimonio de otro a través de una simulación, deformando u ocultando hechos verdaderos, excitando a un error o manteniéndolo, se castiga con"... (traducción del autor).

[16] "El culpable de robo con fuerza en las cosas efectuado en lugar habitado o destinado a la habitación o en sus dependencias, sufrirá la pena de presidio mayor en su grado mínimo si cometiere el delito: 3° Introduciéndose en el lugar del robo mediante la seducción de algún doméstico, o a favor de nombres supuestos o simulación de autoridad".

[17] Véase SIEBER, Ulrich, *Informationstechnologie und Strafrechtsreform*, Köln - Berlin - Bonn - München, Carl Heymanns Verlag KG, 1985, pp. 38 y ss.

[18] Así, LACKNER, Karl, *Zum Stellenwert...,* pp. 51 y ss.

con el § 263[19]. Entonces, para evitar insuficiencias y una expansión sin límites de la norma, se afirma por la doctrina alemana mayoritaria que tiene que valer como regla de interpretación para todas las variantes del tipo, que no se puede aplicar el § 263a, si el comportamiento no se corresponde a un engaño hacia personas como en la estafa[20]. De esto resulta –según la doctrina alemana dominante[21]– que el § 263a quiere comprender sólo los casos en que por falta de una influencia intelectual sobre una persona y de su reacción condicionada por error, no puedan ser comprendidos por el § 263.

Por otro lado, en *Italia* el delito objeto de este trabajo se encuentra regulado en el art. 640 ter[22] de su Código Penal, que fue añadido por el art. 10 de la Ley Nº 547 de 23/12/1993, y se dirige a reprimir las hipótesis de ilícito enriquecimiento conseguidas por el empleo "fraudulento" de un sistema informático. En dicho país se ha manifestado[23] que el fenómeno, bien conocido en los Órdenes de todos los países industrializados, consiste en la interferencia sobre el desarrollo regular de un proceso de elaboración de datos, para conseguir, como resultado de la alteración del resultado de la elaboración, un desplazamiento patrimonial injustificado.

La doctrina italiana ha considerado que la posibilidad de *reconducir* estas hipótesis a la figura de la estafa tradicional (art. 640[24] de su Código Penal), si no pudiera excluirse completamente, resultó en todo caso fuertemente condicionada por las circunstancias del caso concreto: no pudiendo, en efecto, asimilarse la utilización fraudulenta de la máquina al engaño de un hombre –en razón de la prohibición de *analogía en malam*

[19] Así, CRAMER, Peter y PERRON, Walter, *op. cit.,* número de margen 2.

[20] De acuerdo con la interpretación similar a la estafa, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 3; HOYER, Andreas, "§ 263a", en *Systematischer Kommentar zum Strafgesetzbuch*, Band II, BT (§§ 80 - 358), Neuwied, Luchterhand, 2006, número de margen 3; LACKNER, Karl, *Zum Stellenwert...*, pp. 54 ss; LACKNER, Karl y KÜHL, Kristian, "§ 263a", en *Strafgesetzbuch Kommentar*, München, C.H. Beck, 2007, número de margen 13; RENGIER, Rudolf, *Strafrecht, Besonderer Teil I, Vermögensdelikte*, München, C.H. Beck, 2006, § 14, número de margen 2; WESSELS, Johannes y HILLENKAMP, Thomas, Strafrecht, Besonderer Teil/2, Heildelberg, C.F. Müller Verlag, 2007, § 13, número de margen 600; KINDHÄUSER, Urs, *op. cit.*, números de margen 6 y ss.; De otra opinión, MITSCH, Wolfgang, *Strafrecht. Besonderer Teil 2, Teilband 2*, Berlin, Springer, 2001, § 3, número de margen 22; TIEDEMANN, Klaus, *263a…*, número de margen 16.

[21] Así, LACKNER, Karl, *Zum Stellenwert...,* pp. 54 ss.

[22] Esta norma dice: "Fraude informático. Quien, alterando de cualquier modo el funcionamiento de un sistema informático o telemático o interviniendo sin derecho con cualquier modalidad sobre datos, informaciones o programas contenidos en un sistema informático o telemático o a ellos pertinentes, procura para sí o a otro un injusto provecho con daño ajeno, es castigado con privación de libertad de seis meses a tres años y con multa de 51 euros a 1.032 euros. La pena es privativa de libertad de uno a cinco años y de multa de 309 euros a 1.549 euros, si concurre una de las circunstancias previstas por el número 1 del inciso segundo del art. 640, o bien si el hecho es cometido con abuso de la calidad de operador del sistema. El delito es punible a querella de la persona ofendida, salvo que concurra alguna de las circunstancias del inciso segundo u otra circunstancia agravante" (traducción del autor).

[23] Véase PECORELLA, Claudia, "art. 640 ter", en DOLCINI, Emilio e MARINUCCI, Giorgio (a cura di), *Codice Penale Commentato*, Vicenza, Ipsoa, 2006, número de margen 1.

[24] Esta norma señala: "Estafa. Quien, con artificios o insidias, induciendo a alguien en error, procura para sí o a otro un injusto provecho con daño ajeno, es castigado con privación de libertad de seis meses a tres años y con multa de 51 euros a 1.032 euros. La pena es privativa de libertad de uno a cinco años y de multa de 309 euros a 1.549 euros: 1) si el hecho es cometido contra el Estado u otro ente público o con el pretexto de hacer exonerar a alguien del servicio militar; 2) si el hecho es cometido engendrando en la persona ofendida el temor de un peligro imaginario o la errónea convicción de deber ejecutar una orden de la autoridad. El delito es punible a querella de la persona ofendida, salvo que concurra alguna de las circunstancias previstas por el párrafo anterior u otra circunstancia agravante" (traducción del autor).

partem–, fue indispensable verificar si en el caso concreto una persona, antepuesta al control de la elaboración en un momento posterior al que intervino la manipulación, hubiera sido inducida en error a consecuencia de la intervención fraudulenta. Y justo sobre la base de consideraciones de este tenor, es que la jurisprudencia italiana ha aplicado a veces el art. 640[25]. P. ej., en el caso de manipulaciones de datos habientes a objeto de procesos informáticos que previeron todavía el concurso del hombre (eventualidad, ésta, destinada a desaparecer con el progreso de la informatización, que se basa sobre la sustitución integral del computador al hombre)[26].

Para la *mayoría* de la doctrina italiana[27], –como hemos adelantado– el nuevo tipo de *estafa informática* aparece claramente inspirado en el esquema de la estafa, proponiéndose integrar el art. 640 únicamente en aquellos casos en que el computador haya reemplazado el proceso decisional de un ser humano en la valoración de situaciones relevantes sobre el plan económico. Sin embargo, se dice que la *simetría* entre las dos figuras de delito no es *perfecta*[28]: se afirma que al describir la concatenación causal entre las muchas fases en que se articula la agresión al patrimonio ajeno el art. 640 ter no establece el elemento de la inducción en error de la víctima, o sea, en el ámbito informático, la causación de un resultado inexacto, o en todo caso irregular, del proceso de elaboración de datos con respecto del que ha intervenido la manipulación. Tal elemento del tipo ha sido, sin embargo, creído implícito por el intérprete, para asegurar a la norma sobre la *estafa informática* un ámbito de operatividad circunscrito a las hipótesis en las que habría sido aplicable la norma de la estafa tradicional, si solamente la conducta fraudulenta se hubiera dirigido a una persona, en vez de a un computador[29].

Finalmente, el art. 248.2 a)[30] del Código Penal español nació al mismo tiempo que el Código Penal de 1995[31]. En ese país la mayoría de la doctrina estima que el delito de estafa clásico o tradicional implica una relación directa y personal entre dos seres humanos, y le otorga al error la condición de elemento autónomo. Esta realidad hizo necesaria la creación de un nuevo delito de "estafa informática".

En España la doctrina mayoritaria concibe al delito objeto de este trabajo como una

[25] Confróntese sentencias del Tribunal de Roma de 14/12/1985 y de 20/06/1985 (citadas por PECORELLA, Claudia, *"art. 640 ter"*, número de margen 2).

[26] En doctrina, desearon una intervención del legislador para reprimir estas hipótesis particularmente insidiosas de agresión patrimonial, FIANDACA, Giovanni, MUSCO, Enzo, *Diritto penale, Parte speciale, I delitti contro il patrimonio*, Bologna, Zanichelli editore, 2005, vol.II, II, p. 196; y, por todos los que creyeron, en cambio, que era posible reconocer en todo caso el engaño de una persona, y por lo tanto, aplicar la estafa tradicional, véase PIOLETTI, Ugo, voz "Truffa", en *Novissimo Digesto Italiano*, 1987, pp. 911 y ss.

[27] Confróntese, por todos, FANELLI, Andrea, *La truffa*, Milano, Giuffrè, 1998, p. 414; PICA, Giorgio, *Diritto penale delle tecnologie informatiche*, Turín, Utet, 1999, pp. 143 y ss.

[28] Véase, por todos, FIANDACA, Giovanni, MUSCO, Enzo, *op. cit.*, pp. 196-197; ANTOLISEI, Francesco, *Manuale di Diritto Penale, Parte speciale, a cura di Luigi Conti*, Milano, Multa Pavcis, 2002, I, pp. 374-375.

[29] Así, PECORELLA, Claudia, *art. 640 ter…*, número de margen 3.

[30] "También se consideran reos de estafa: a) Los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro".

[31] L.O. 10/1995, de 23 de noviembre (BOE 24/11/1995, número 281; rectificación, BOE 2/03/1996, número 54).

estafa impropia; o, como una estafa general, pero con rasgos que dificultan una equivalencia completa con el delito de estafa clásico o tradicional.

Sentadas estas pequeñas bases, ahora nos adentraremos en el análisis del tipo de *estafa informática*, a la luz de los arts. 263a del Código Penal Alemán; 640 ter del Código Penal italiano; y, 248.2 a) del Código Penal español[32].

III. EL MODELO "EXHAUSTIVO" ALEMÁN DEL § 263A DEL CÓDIGO PENAL ALEMÁN

1. Conducta típica: "incorrecta configuración del programa"; "utilización de datos incorrectos o incompletos"; "utilización no autorizada de datos"; y, "cualquier otra forma de influencia no autorizada en el proceso de tratamiento de datos"

Creemos que resulta muy *importante* en la interpretación del tipo de *estafa informática* tener presente cómo se comprende al mismo en Alemania. Sobran las palabras para justificar esta observación, pero, debe hacerse hincapié en que en dicho país las más de dos décadas de tipificación de nuestro delito, unido al hecho de que siempre es un referente en *nuevas tecnologías*, constituyen motivos sufientes para tener presente a este Derecho a la hora de discutir los límites de la *estafa informática*[33].

El Código Penal Alemán utiliza un sistema *exhaustivo* con el propósito de evitar cualquier tipo de *vacíos legales*[34]. Según su § 263a, "*Quien, con el propósito de obtener una ventaja patrimonial antijurídica para sí o para un tercero, perjudica el patrimonio de otro, influyendo en el resultado de un proceso de tratamiento de datos, a través de una errónea configuración del programa, a través del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos, o de otra manera a través de una intervención no autorizada en el proceso, se castiga con privación de libertad de hasta cinco años o con multa*" (la traducción es nuestra).

De la lectura de esta norma se puede desprender que el § 263a contempla *cuatro* posibles diferentes *modalidades* comisivas, que se pueden enumerar de la siguiente forma:

[32] En el Derecho europeo continental, los sistemas legislativos sobre la estafa informática se dividen entre aquellos países que efectúan una descripción exhausta (e incluso, enumerativa) de las modalidades comisivas (como ocurre en Alemania o Portugal); y aquellos que utilizan definiciones generales (como es el caso de Italia y España). Sobre las formas de tipificación de la estafa informática en Derecho comparado, véase GUTIÉRREZ FRANCÉS, Mª Luz, *Fraude informático y estafa*, Madrid, Ministerio de Justicia, 1991, pp. 117 y ss.; ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Granada, Comares, 2002, pp. 341 y ss.; GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos*, Valencia, Tirant lo Blanch, 2005, pp. 59 y ss.

[33] Otro referente en esta materia debería ser el Derecho de los *Estados Unidos*. No obstante, no hemos incluido a dicho país en nuestra investigación, por tratarse de una tradición jurídica muy diferente a la nuestra (GALÁN MUÑOZ, Alfonso, *El fraude..., op. cit.*, pp. 70 y ss.; ROVIRA DEL CANTO, Enrique, *op. cit.*, pp. 345 y ss.; GUTIÉRREZ FRANCÉS, Mª Luz, *Fraude informático…,* pp. 119 y ss.).

[34] Así, TIEDEMANN, Klaus, *263a…*, números de margen 1 y ss.

(a) Incorrecta configuración del programa (primera variante);
(b) Utilización de datos incorrectos o incompletos (segunda variante);
(c) Utilización no autorizada de datos (tercera variante); y,
(d) Cualquier otra forma de influencia no autorizada en el proceso de tratamiento de datos (cuarta variante).

Los *hechos punibles*[35] –las cuatro variantes–, que son parcialmente recreados en aquéllos descritos en el delito de estafa clásico (p. ej., uso de datos incorrectos = afirmación de hechos incorrectos), deben comprender todos los tipos de manipulación que puedan influir en el resultado del proceso de tratamiento de datos[36]. Seguidamente, estudiaremos cada una de estas *variantes*.

La *primera variante* del § 263a consiste en la "configuración incorrecta del programa"[37]. A estos efectos, se tiene que entender por "programa" las instrucciones de trabajo en un computador que se componen de una consecuencia de comandos individual (denominada "etapas de marcha del programa")[38].

Es menester apuntar que *no existe* una única respuesta respecto a qué debe entenderse por un programa configurado de forma incorrecta:

i) Para la *doctrina dominante*, esto debe comprenderse de forma "objetiva"[39], esto es, efectuando una comparación entre el tratamiento realizado y el resultado finalmente obtenido con el mismo y aquellos (tratamiento y resultado) que no se deberían haber producido en el sistema mediante el uso de datos correctos;

[35] Sobre su relación, confróntese TIEDEMANN, Klaus, *263a…*, número de margen 24.

[36] Así, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 4.

[37] Sobre este primer punto, brevemente, nos gustaría apuntar que esta modalidad versa sobre las denominadas "manipulaciones del programa" (Véase, por todos, ARZT, Gunther y WEBER, Ulrich, *Strafrecht, Besonderer Teil*, Bielefeld, Verlag Ernst und Werner Gieseking, 2000, § 21, número de margen 32) y, según la mayoría de la doctrina alemana, se comprende que los programas informáticos no mantienen una autonomía conceptual con respecto al concepto de "dato", estimando, en tal dirección, que los programas siempre están compuestos por datos, e inclusive, se afirma que "son datos". Con ello, ambos conceptos no se configuran como realidades ontológicamente diferentes e independientes la una de la otra, circunstancia que no dota, a su vez, de razón de ser a la existencia e independencia de las modalidades típicas referidas a los mismos, haciendo que se pueda estimar que esta modalidad es simplemente "aclarativa", pero, también, funciona como una especialidad respecto de la segunda modalidad (por todos, véase TIEDEMANN, Klaus, *263a…*, número de margen 27; WESSELS, Johannes y HILLENKAMP, Thomas, *op. cit.,* § 13, número de margen 606).

[38] Así, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 5.

[39] Por todos, HOYER, Andreas, *op. cit.*, número de margen 24; LACKNER, Karl, *Zum Stellenwert...,* pp. 55 ss; LACKNER, Karl y KÜHL, Kristian, *§ 263a…,* número de margen 7; MAURACH, Reinhart, SCHROEDER, Friedrich-Christian y MAIWALD, Manfred, *Strafrecht, Besonderer Teil, Teilband 1*, Heildelberg, C.F. Müller Verlag, 2003, § 41, número de margen 231; RENGIER, Rudolf, Strafrecht..., *op. cit.*, § 14, número de margen 4; TIEDEMANN, Klaus, *263a…*, número de margen 31; TIEDEMANN, Klaus, *Wirtschaftsstrafrecht. Besonderer Teil mit wichtigen Gesetzes- und Verordnungstexten*, München, Carl Heymanns Verlag, 2008, § 10, número de margen 481; FISCHER, Thomas, *Strafgesetzbuch und Nebengezetse*, München, C.H. Beck, 2008, § 263a, número de margen 6; WESSELS, Johannes y HILLENKAMP, Thomas, *op. cit.*, § 13, número de margen 606; HILGENDORF, Eric, FRANK, Thomas y VALERIUS, Brian, Computer- und Internetstrafrecht, Berlin, Springer, 2005, número de margen 139.

ii) Para la *opinión minoritaria* (subjetiva), por su parte, un programa es "incorrecto" cuando no corresponde la voluntad del autorizado para disponer con la formación de las ideas[40]. Sostienen que la opinión contraria, que, como vimos, se refiere a la *objetiva* tarea del proceso de tratamiento de datos, ignoraría que la "corrección" del programa, con independencia de la voluntad del gestor del programa, no puede existir. Al contrario –dicen–, éste fija libremente sus metas a establecer y, entonces, o bien elige dentro del *software* estándar existente, y si requiere de necesidades específicas, que se correspondan mejor con sus especificaciones, se ajusta a ellas, o bien crea el programa correspondiente o, lo encarga[41].

No obstante, la *importancia práctica* de la disputa es, al parecer, pequeña[42].

La *manipulación del programa* puede ser, o bien *conforme* al sistema, o bien *contraria* al sistema. En el *primer caso*, se influiría en la marcha del programa elaborado por el autorizado a disponer, p. ej., con la instalación de etapas de marcha del programa adicionales o si se cambian etapas de marcha del programa individuales; si se borra; o, si evita a través de ramificaciones electrónicas. Se podría alcanzar esto, p. ej., sin que los datos se introduzcan o si son transformados de forma diferente a la que el autorizado para disponer hubiera previsto. A través de la manipulación del programa *contraria* al sistema, no se alterarían las etapas de marcha del programa inmanentes, sino las existentes con anticipación que se hayan superpuesto. Así se pueden evitar, p. ej., los controles montados para el impedimento de manipulaciones informáticas[43].

Finalmente, la "programación incorrecta" incluye asimismo casos de "manipulación de operación" en el sentido del "efecto sobre el resultado", así como las manipulaciones del *input*, que se dejarían comprender también como influencias a través de la puesta en práctica de los datos incorrectos o incompletos[44].

La *segunda variante* del § 263a representaría de forma más clara el paralelo con el engaño de la estafa tradicional[45], consiste en el "uso de datos incorrectos o incompletos"[46]. Para el concepto de "dato" –a estos efectos– debemos tener presente, en primer lugar, que *no es unívoco*[47]. En efecto, la definición que sigue la *mayoría de la doctrina alema-*

[40] Confróntese, por todos, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 5; KINDHÄUSER, Urs, "§ 263a", *op. cit.*, números de margen 14 y ss., y 21; MITSCH, Wolfgang, Strafrecht..., *op. cit.*, § 3, número de margen 17.

[41] Así, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 5.

[42] Véase KINDHÄUSER, Urs, *op. cit.*, número de margen 23; MITSCH, Wolfgang, *op. cit.*, § 3, número de margen 18.

[43] Así, TIEDEMANN, Klaus, *263a…*, número de margen 28.

[44] Confróntese CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 5.

[45] Así, TIEDEMANN, Klaus, *Wirtschaftsstrafrecht. Besonderer…*, § 10, número de margen 482.

[46] Sobre este asunto, brevemente, tenemos que decir que esta modalidad versa sobre las denominadas "manipulaciones del input" (Véase, por todos, ARZT, Gunther y WEBER, Ulrich, *op. cit.*, § 21, número de margen 32; CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 6).

[47] Véase LENCKNER, 2006, número de margen 3.

na[48] es aquella que tiene en cuenta –pero no de forma absoluta– al art. 202a (2)[49] del Código Penal Alemán –referido al *espionaje de datos*– y a la norma DIN 44300-2 –emitida por el Instituto Alemán para la normalización de la industria–. En este sentido, la *doctrina dominante* comprende por "dato", aquella representación de informaciones en las cuales se efectúa la representación por signos o funciones continuas, por "datos incorrectos", aquellos que no se corresponden con la realidad, resultando, de tal manera, la información de los mismos falsa; y, por "datos incompletos" aquellos que no dejan conocer suficientemente el supuesto de la realidad.

Por su parte, Hilgendorf , Frank y Valerius[50] estiman que el concepto de dato es más amplio que el que se contiene en el art. 202a, pues en su opinión no se limita a los datos que no sean perceptibles "inmediatamente".

Finalmente, se ha manifestado que los datos son "utilizados" si *contribuyen* al aparato de procesamiento de datos[51]. No se comprendería en este concepto, por tanto, la mera fabricación de los llamados "documentos fuente" no *legibles* por las máquinas (p. ej., facturas). Sin embargo, quien fabrica "documentos fuente" con conocimiento de que serán empleados de buena fe, cometería el hecho en *autoría mediata*. Asimismo, si al instrumento se le confía la revisión objetiva del contenido de los datos, se descartaría así la autoría mediata[52]. Además, en los casos pertenecientes a esta modalidad del hecho, los datos introducidos se llevarían a otro contexto o se suprimirían. El ámbito de aplicación de este elemento no debería restringirse a los "datos no directamente perceptibles", de modo diferente al § 202a, en el sentido de poder abarcar también los datos del *input* que todavía no hayan sido almacenados[53].

La *tercera variante* del § 263a consiste en el "uso no autorizado de datos"[54]. Esta modalidad no versa sobre una *influencia* adversa del programa u objetivamente incorrecta de un proceso de tratamiento de datos, sino sobre el *propósito* antijurídico de influir en una operación informática autorizada mediante datos "correctos" a través de personas que no están autorizadas para ello, o que aprovechen su posibilidad de entrada al com-

[48] Véase, por todos, TIEDEMANN, Klaus, *263a…*, números de margen 19, 32 y ss. En sentido similar, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 7, quiénes se remiten literalmente al art. 202a del Código Penal alemán para el concepto de datos, pero en el resto siguen la misma postura.

[49] "(1) Quien, sin autorización procure para sí o para otro datos que no le correspondan y que estén especialmente protegidos contra su acceso no autorizado, será castigado…. (2) Datos en el sentido del apartado 1, únicamente son aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente accesible" (traducción del autor).

[50] HILGENDORF, Eric, FRANK, Thomas y VALERIUS, Brian, *op. cit.*, número de margen 141.

[51] Así, KINDHÄUSER, Urs, *op. cit.*, número de margen 24; LACKNER, Karl y KÜHL, Kristian, *§ 263a…,* número de margen 9.

[52] Confróntese TIEDEMANN, Klaus, *263a…*, números de margen 36, 38; HOYER, Andreas, *op. cit.,* número de margen 27.

[53] Así, FISCHER, Thomas, *op. cit.*, § 263a, número de margen 7.

[54] Esta tercera modalidad comisiva del delito de estafa informática, constituye el *principal* elemento delimitador de la misma en Alemania (es decir, se erige como la modalidad más importante), aquel que viene a establecer el requerimiento de que los comportamientos comprensibles en la misma tuviesen la naturaleza de "no autorizados" (véase GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 131).

putador con propósitos antijurídicos[55].

Esta alternativa fue propuesta por la *Comisión Jurídica del Parlamento Alemán* con la finalidad de poder abarcar el uso abusivo de *tarjetas* de código en cajeros automáticos[56]. Particularmente, la obtención de dinero en efectivo por una persona no autorizada con ayuda de una tarjeta de código extraña y su correspondiente número secreto, debería ser acogida en el tipo del § 263a. Así, el *resultado* del proceso de tratamiento de datos no sólo se *influiría* si se evidencia como contenido incorrecto en forma de contradicción entre el estado del activo y del pasivo, sino también, si su realización depende del uso de datos *no autorizado*[57]. Sin embargo, de acuerdo con la *redacción* del texto de la norma, la hipótesis alcanzaría también a aquellos casos en los cuales el beneficiario saca dinero en efectivo del cajero automático rebasando su límite de crédito. No obstante, la punibilidad de este comportamiento, es sumamente dudosa, pues tal abuso puede ser evitado, ampliamente hoy en día, a través de protecciones técnicas. A causa de esto, y con respecto a otros grupos de casos, se ha dicho que se requiere aquí una medida especial de interpretación *restrictiva*[58].

Por un lado, esto es *aplicable* para el uso de datos que presuponen también en esta variante del tipo que los datos se aportarían en el proceso de tratamiento de datos y que el aparato sólo procesa a éstos y a ningún otro dato, de acuerdo con la *voluntad* del autor[59]. El curso de una máquina traga monedas se vuelca a través de una simulación informática, p. ej., exactamente después de presionar el "botón de riesgo", donde se espera que la máquina acto seguido con los fundamentos de este conocimiento, sistemáticamente pierda, y así la verdad es que el autor se aprovecharía de los conocimientos sobre los datos contenidos en el *software* de la máquina, pero, sin embargo, no "usa" esos datos[60].

Particularmente, se tiene que exponer a este elemento *restringiéndolo* de forma "no autorizada".

Esto es un *componente* del tipo y no una mera observación referente a su ilegalidad como característica general del delito, porque el carácter de injusto específico sólo se manifiesta en esta variante del tipo[61]. Se ha expresado que cada contacto con los datos no es suficiente, pues debe contradecirse la voluntad verdadera o supuesta del autorizado para disponer[62].

---

[55] Véase CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 7.

[56] Confróntese SIEBER, Ulrich, *Informationstechnologie und...*, p. 38.

[57] Confróntese WESSELS, Johannes y HILLENKAMP, Thomas, *op. cit.*, § 13, número de margen 608.

[58] Así, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 7.

[59] Véase KINDHÄUSER, Urs, "§ 263a", *op. cit.*, número de margen 28.

[60] De esta opinión, MITSCH, Wolfgang, *Strafrecht...*, *op. cit.*, § 3, número de margen 25; RENGIER, Rudolf, *Strafrecht...*, *op. cit.*, § 14, número de margen 14; WESSELS, Johannes y HILLENKAMP, Thomas, *op. cit.*, § 13, número de margen 612; ARZT, Gunther y WEBER, Ulrich, *op. cit.*, § 21, número de margen 47; HOYER, Andreas, *op. cit.*, número de margen 45; TIEDEMANN, Klaus, *263a…*, números de margen 21 y 61; CRAMER, Peter y PERRON, Walter, *op. cit.*, números de margen 8 y 17.

[61] Así, KINDHÄUSER, Urs, *op. cit.*, número de margen 28; FISCHER, Thomas, *op. cit.*, § 263a, número de margen 10.

[62] Confróntese MAURACH, Reinhart, SCHROEDER, Friedrich-Christian y MAIWALD, Manfred, *op. cit.*,

A causa de la orden de *interpretación similar a la estafa*, sería más bien necesario que la acción de una situación de engaño se corresponda con la estafa clásica o tradicional, es decir, que en el caso de uso de los datos frente a una persona estaría explicado, por lo menos concluyentemente, la autorización del uso[63]. Las exigencias adicionales demandan, en el sentido de una interpretación "específicamente informática", que la autorización para usar los datos del programa deba ser comprobada por el mismo *software*[64], y conducirían, por otro lado, a una limitación no buscada por el legislador y no justificada también objetivamente en el tipo, motivo por el cual parece que se tiene que rechazar[65].

En conclusión, la *mayoría de la doctrina alemana*[66] se ha inclinado por comprender que la disposición del uso de datos no autorizados resulta tan relevante en la descripción típica del delito de *estafa informática*, que carecería de contenido de injusto un uso de datos "autorizado", lo que obligaría a estimar que tal exigencia es esencial para afirmar la tipicidad del delito. Asimismo, debe decirse que ha sido objeto de gran *polémica* la voz "no autorizado" que tiene que utilizarse a estos efectos, decantándose la *doctrina mayoritaria* por buscar la restricción de este elemento por medio del requerimiento de que las conductas que pudiesen verse comprendidas mantengan un cierto *paralelismo* con el delito de estafa clásico o tradicional, postura que, al mismo tiempo, permitiría solventar los posibles eventos de aplicación del art. 266 (I)[67] del Código Penal Alemán, que regula el delito de *infidelidad*. El paralelismo mencionado, a su vez, tampoco se interpreta de la *misma forma*, y así nos encontramos con algunos que fundamentaban su interpretación en el hecho de que debe considerase existente un "paralelismo estructural"; mientras otros estiman que las modalidades comisivas del delito de *estafa informática* siempre deberían tener un "contenido de desvalor equiparable al engaño típico de la estafa" –esta última es la *doctrina dominante*– (lo que es sumamente importante para comprender la naturaleza del delito de *estafa informática*). En este último sentido,

§ 41, número de margen 232; MITSCH, Wolfgang, *op. cit.*, § 3, número de margen 23; TIEDEMANN, Klaus, *263a…*, número de margen 43.

[63] Por todos, véase LACKNER, Karl y KÜHL, Kristian, *§ 263a…,* número de margen 13; RENGIER, Rudolf, *Strafrecht...*, *op. cit.*, § 14, número de margen 12; FISCHER, Thomas, *op. cit.*, § 263a, número de margen 11; WESSELS, Johannes y HILLENKAMP, Thomas, *op. cit.*, § 13, número de margen 609; KINDHÄUSER, Urs, "§ 263a", *op. cit.*, números de margen 29, 35 y ss.; TIEDEMANN, Klaus, *Wirtschafisstrafrecht. Besonderer…*, § 10, número de margen 475; CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 9. De otra opinión, LACKNER, Karl, *Zum Stellenwert...,* p. 53, MITSCH, Wolfgang, *op. cit.*, § 3, número de margen 23.

[64] Así, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 9.

[65] Véase KINDHÄUSER, Urs, *op. cit.*, número de margen 34; TIEDEMANN, Klaus, *263a…*, número de margen 45.

[66] Confróntese, sobre estos problemas, y por quienes siguen la postura mayoritaria, TIEDEMANN, Klaus, *263a…*, números de margen 40 y ss.; TIEDEMANN, Klaus, *Wirtschafisstrafrecht. Besonderer…*, § 10, número de margen 475; CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 11; HILGENDORF, Eric, FRANK, Thomas y VALERIUS, Brian, *op. cit.*, número de margen 144.

[67] Este art. dice: *"Quien abusa de la facultad concedida a través de la ley, o por una orden de autoridad o por un negocio jurídico, para disponer de un patrimonio ajeno u obligar a otro; o quien quebrante el deber de salvaguardar los intereses patrimoniales ajenos derivados de la ley o de una orden de autoridad o por negocio jurídico o por una relación de fidelidad, y con ello ocasione una desventaja a la persona cuyos intereses debe cuidar, será castigado…"* (traducción del autor).

únicamente se podría considerar un "uso no autorizado de datos", asimilable o análogo al engaño del delito de estafa, y por lo tanto, "típico", cuando la mera realización del negocio jurídico ya signifique la "declaración tácita" de que se estaba llevando a cabo con autorización, desde el punto de vista del tráfico jurídico, aun cuando el autor no haya efectuado ninguna declaración expresa.

Por último, la *cuarta variante* del § 263a versa sobre "cualquier otra forma de influencia no autorizada sobre el proceso"[68]. Esta modalidad del hecho, se ha dicho que con referencia al art. 103 párrafo 2[69] GG –que consagra el principio de legalidad–, se encuentra formulada de modo muy *indeterminada*[70], al utilizar la voz "de otra manera" o "de cualquier forma"[71-72].

Según la *historia fidedigna* de la ley, las palabras "efecto sobre el proceso" deberían asegurar que se comprendan las especialmente peligrosas manipulaciones en la consola, que no siempre presuponen datos incorrectos, y que de cualquier manera influyan en la instrucción para el proceso de tratamiento de datos o cambien el proceso automático del programa[73].

El elemento insertado más tarde "no autorizada", es, como en el caso de la tercera variante del tipo, un elemento que constituye el contenido de injusto del comportamiento, y una peculiaridad del delito, no solamente general[74].

En vista de lo *abierto* e *indefinido* del "efecto en el proceso", se utiliza como medida especial de *delimitación* técnica y como limitación de esta variante del tipo, a los casos efectivamente dignos de penalidad y referidos a los que quiso incriminar el legislador, y, por ello, se tiene que exponer *restrictivamente*, como en el caso de la tercera variante, de manera específica en correspondencia con la estafa[75].

---

[68] Sobre esta modalidad comisiva, existe *acuerdo* doctrinal en considerar que tiene por función la de servir de *cláusula de cierre* de las eventuales lagunas de punibilidad que pudiesen presentar las anteriores; señalándose al efecto que posibilita la consideración como constitutivas del delito de estafa informática aquellas eventuales influencias en el desarrollo del proceso de datos, que no hubiesen atribuido una verdadera alteración en la configuración del programa informático en cuestión, como podrían resultar las manipulaciones del *hardware* y del *output*, constituyendo igualmente un instrumento adecuado para lograr la reacción penal frente a todas aquellas manipulaciones que se pudiesen llegar a originar como producto del desarrollo tecnológico (Véase, por todos, TIEDEMANN, Klaus, *263a…*, número de margen 62; TIEDEMANN, Klaus, *Wirtschafsstrafrecht. Besonderer…*, § 10, número de margen 489, donde dice que en esta modalidad no es necesaria la similitud con el engaño de la estafa; CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 12; HILGENDORF, Eric, FRANK, Thomas y VALERIUS, Brian, *op. cit.*, número de margen 151; WESSELS, Johannes y HILLENKAMP, Thomas, *op. cit.*, § 13, número de margen 612; RENGIER, Rudolf, *Strafrecht...*, *op. cit.*, § 14, números de margen 7 y 13).

[69] "Un acto sólo se puede castigar si la pena estaba prevista por ley antes de que se cometiera" (traducción del autor).

[70] Véase KINDHÄUSER, Urs, *op. cit.*, número de margen 63.

[71] Así, TIEDEMANN, Klaus, *263a…*, número de margen 24; FISCHER, Thomas, *op. cit.*, § 263a, número de margen 18.

[72] En alemán, lo que se cuestiona es la voz *"sonst"*, que literalmente significa "de lo contrario", "si no", "por lo demás", "además". Entonces, al no encontrar una expresión exacta en castellano, creímos pertinente utilizar las locuciones citadas.

[73] Así, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 16.

[74] Confróntese KINDHÄUSER, Urs, *op. cit.*, número de margen 64; FISCHER, Thomas, *op. cit.*, § 263a, número de margen 18.

[75] Así, TIEDEMANN, Klaus, *"§ 263a"*, números de margen 62-63; FISCHER, Thomas, *op. cit.*, § 263a,

2. Resultado típico: "la influencia en el proceso de tratamiento de datos"

El hecho punible (es decir, cualquiera de las cuatro variantes[76]) tiene que *influir en el proceso de tratamiento de datos informáticos*[77]. Esto significa que el autor influye de tal manera que se llega a cambiar el resultado de los datos almacenados en el computador, y el de aquellos que sean utilizados por el programa de trabajo. No juega ningún papel si se pone en marcha un nuevo proceso de tratamiento de datos, o si influye en uno ya existente[78]. Sobre este elemento, se señala en la *historia fidedigna de la ley*, que la influencia sobre el resultado de un proceso de tratamiento de datos se refiere a aquellos *casos* en que el autor no se sirve de un computador, sino que influye en una persona, p. ej., en el resultado de un proceso de pensar y decidir, y esta paráfrasis cubriría, en relación con el tipo de estafa, tanto la disposición patrimonial como el error. Corresponde al proceso de pensar y decidir erróneo el proceso de tratamiento de datos determinado que conduzca a la utilización de los medios mencionados en el tipo, forzando técnicamente a un resultado falso, donde, sin embargo, se comprende la no mencionada –en Alemania– "disposición patrimonial" del tipo de estafa. Por esto, este elemento, en relación con el propósito de enriquecimiento exigido en el tipo subjetivo, hace que el § 263a también sea un delito de *desplazamiento patrimonial*. En el lugar de la disposición patrimonial condicionada por error, exigida para el § 263, va la potencialidad del computador falsificada por el autor que conduce a una desventaja del interesado[79].

Para terminar, a partir de esto, por tanto, se tiene que *concluir* que la clara intención del legislador alemán es que, en todo caso, el abuso de tarjetas bancarias, de otras tarjetas de código, y de procedimientos técnicos de pago similares, se tengan que juzgar exclusivamente acorde al § 263a, pues el engaño del concepto de estafa acontece exactamente con referencia a este tipo de constelaciones[80]. Por lo tanto, la obtención de dinero en efectivo por el no autorizado, sobre instalaciones técnicas de este tipo, se comprendería únicamente por el § 263a como ley especial[81].

número de margen 18.

[76] Así, TIEDEMANN, Klaus, *Wirtschaftsstrafrecht. Besonderer*…, § 10, número de margen 490, donde además indica que esta consecuencia intermedia, con admisión del perjuicio patrimonial, va en lugar del error y del acto de disposición; y, exige causalidad.

[77] Véase CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 18.

[78] Confróntese KINDHÄUSER, Urs, *op. cit.*, número de margen 69; MITSCH, Wolfgang, *op. cit.*, § 3, número de margen 27; FISCHER, Thomas, *op. cit.*, § 263a, número de margen 20.

[79] Así, CRAMER, Peter y PERRON, Walter, *op. cit.*, número de margen 18.

[80] Así, HOYER, Andreas, *op. cit.*, números de margen 42 y 64; TIEDEMANN, Klaus, *263a.*…, número de margen 84.

[81] Véase TIEDEMANN, Klaus, *263a.*…, número de margen 84.

IV. EL MODELO DE "DEFINICIÓN GENERAL" DEL ART. 640 TER CÓDIGO PENAL ITALIANO

1. Conducta típica: la "alteración de cualquier modo del funcionamiento de un sistema informático o telemático" o la "intervención sin derecho con cualquier modalidad sobre datos, informaciones o programas"

Otro referente obligado en nuestra órbita de cultura es el Derecho italiano. Por este motivo ilustraremos como la doctrina y jurisprudencia de ese país interpretan al delito objeto de nuestro trabajo de investigación.

En Italia, utilizando el sistema de definiciones generales, el delito de *estafa informática* se encuentra regulado en el art. 640 ter de su Código Penal, cuyo párrafo primero señala: "*Quien, alterando de cualquier modo el funcionamiento de un sistema informático o telemático o interviniendo sin derecho con cualquier modalidad sobre datos, informaciones o programas contenidos en un sistema informático o telemático o a ellos pertinentes, procura para sí o a otro un injusto provecho con daño ajeno, es castigado con privación de libertad de seis meses a tres años y con multa de 51 euros a 1.032 euros*" (la traducción es nuestra).

La conducta "fraudulenta" tiene que consistir en alterar, de cualquier modo, el funcionamiento de un sistema informático, o bien en intervenir, con cualquier modalidad, sobre determinadas informaciones o programas contenidos en el sistema o a ellos pertinentes[82]. A pesar de su *aparente* latitud, la previsión parece resultar, en realidad, precisa y circunscrita, ya sea si se confrontara con la genérica previsión de los "artificios e insidias" de la estafa tradicional del art. 640 del Código Penal italiano, ya sea si se considerara en relación al requisito, implícito, de la causación de un resultado irregular del proceso de elaboración como paso obligatorio para llegar al daño patrimonial[83].

El *primer* tipo de intervención "fraudulenta" que menciona la norma en examen tiene por objeto "el funcionamiento de un sistema informático o telemático", y consiste en una modificación del desarrollo regular del proceso de elaboración y/o de transmisión de datos realizado por un "sistema informático o telemático"[84].

También *constituye* un "sistema informático", en el sentido del art. 640 ter del Código Penal italiano, aquéllos *aparatos* que *proveen bienes o servicios* que sean administrados por un computador. Es el caso, p. ej., de todos aquellos aparatos, como máquinas de fotocopias, teléfonos, distribuidores automáticos de billetes, etc., que funcionan a través de tarjetas magnéticas. Estos sistemas trabajan un trato informático de datos, en cuanto el computador en ellos contenidos es capaz –gracias a las instrucciones recibidas– de

[82] Cree que es única la modalidad de comisión de estafa informática, ya siendo la conducta consistente en la intervención sin derecho sobre datos, informaciones y programas comprendidas en la hipótesis de alteración del funcionamiento del sistema, en cuanto ello constituiría una simple especificación ejecutiva, PICA, Giorgio, *op. cit.*, pp. 143 ss.

[83] En este sentido, PICA, Giorgio, *op. cit.*, p. 144.

[84] Confróntese PECORELLA, Claudia, *art. 640 ter…*, número de margen 6.

leer las informaciones memorizadas sobre la adecuada tarjeta magnética, que certifican la legitimación del usuario a recibir la prestación, elaborarla y modificarla, borrando de ellos algunos y/o añadiendo otros, p. ej., la suma de gasto ya utilizada y, por lo tanto, a aquel restante[85].

Se dice que rebosa el *alcance* de la norma incriminatoria aquellos sistemas informáticos que, en sustitución de las tradicionales cerraduras, asumen una *función* de mera protección. Es el caso, p. ej., de los mecanismos electrónicos de apertura y cierre, los que incluso, a veces, obran a través de tarjetas magnéticas. La referencia a estas *barreras* tecnológicas no comportaría, de este modo, de por sí un provecho injusto por el agente, pero hace solamente posible la consiguiente conducta de agresión al patrimonio ajeno[86].

La "alteración" del funcionamiento del sistema debe ocurrir "de cualquier modo" y tiene que ser, por lo tanto, la consecuencia de una intervención relativa, ya sea al *componente mecánico* del computador –p. ej., la manumisión del aparato que sirve para la encuesta directa de los datos a someter a elaboración, o bien la manumisión de la impresora con la que, una vez acabada la elaboración, los datos, es emitida en forma comprensible por la mente y el ojo humano–, ya sea a su *componente lógico*, o sea, al *software*[87].

Entre las *intervenciones* relativas al componente lógico de un sistema informático, son capaces de determinar una alteración del funcionamiento del sistema las manipulaciones del programa, que pueden realizarse por la modificación de algunos de los pasos lógicos previstos en un programa original[88], sea normalmente utilizando un programa diferente o ulterior, con respecto al que se encuentra en uso en un determinado sistema informático. Se ha manifestado que es comprensible en esta hipótesis la conducta consistente en utilizar una línea telefónica interna, sólo habilitada a algunas llamadas previamente programadas, para efectuar llamadas intercontinentales a través de la digitación rápida de una secuencia de números capaz de hacer ineficaz el sistema de protección con que es dotado el aparato telefónico. La manipulación, además, podrá realizarse por medio de un programa "contrario" al sistema, es decir, que no se limita a ejecutar operaciones diferentes de aquellas presupuestadas por el titular del sistema (o, en todo caso, de su legítimo usuario), pero que actúa en un sentido contrario al programa regular, alterándolo o paralizando algunas de sus funciones[89].

Por otra parte, con la fórmula "intervención sin derecho sobre datos, informaciones o programas" se ha dado relevancia a cada forma de interferencia, directa e indirecta, en un proceso de elaboración de datos, diferente de la alteración del funcionamiento del

[85] Así, PECORELLA, Claudia, *art. 640 ter…*, número de margen 7.
[86] Véase PECORELLA, Claudia, *art. 640 ter…*, número de margen 8.
[87] Así, FANELLI, Andrea, *op. cit.*, pp. 415 ss.
[88] Hipótesis comprendida también en la segunda clase de conducta fraudulenta formulada por el art. 640 ter, implicando una "intervención sin derecho" sobre el programa.
[89] Así, PECORELLA, Claudia, *art. 640 ter…,* número de margen 10.

sistema informático[90]. Se vuelve a comprender, entonces, en esta previsión a las manipulaciones del *input* (con las que ha sido hasta hoy realizada la mayor parte de estafas informáticas de que se ha tenido conocimiento), las manipulaciones del programa, y, las manipulaciones del *output* (sea como intervención en la fase de la emisión, en cualquier forma, del resultado de la ya concluida elaboración, sea como intervención sobre el resultado mismo, pero que sea destinada a la consiguiente elaboración, de parte del mismo o de otro computador)[91].

Objeto de la intervención sin derecho pueden ser tanto los *componentes lógicos* del sistema informático, o sea, los "datos"[92] y "programas"[93], como las "informaciones" (que deben entenderse como "informaciones contenidas sobre soportes materiales"[94]). Por la expresa mención de las "informaciones" se comprenderían en el ámbito de la *estafa informática* hipótesis que habrían sido atribuibles, en la mayoría de los casos, al tipo de estafa tradicional (en cuanto a que la información contenida sobre un soporte material [de tarjeta o de otro tipo] sea destinada a ser tratada por el hombre y no [todavía] por la máquina), pero pudieron en algún caso quedar impunes, cuando la información no fuera objeto de ningún control por parte de la persona encargada de trasladar el contenido sobre respaldos idóneos a la lectura por parte del computador (cintas o discos magnéticos, ópticos, etc.)[95].

En esta dirección, de forma general y para explicar la *ratio* del asunto, Pica[96] apunta las siguientes ideas: para ser utilizado por un computador el dato tiene que ser "codificado", es decir representado según un "código" que pueda ser leído y comprendido por el computador, y éste es precisamente el código binario, el alfabeto del computador, compuesto por dos símbolos (bit): 0 y 1.1, símbolos del lenguaje escrito, sean ellos alfabéticos, o bien, numéricos, o gráficos en forma elemental. Asimismo, el autor citado señala que el concepto de "dato" expresa, por lo tanto, una grabación elemental en la memoria de un computador, incluso no teniendo aún su dimensión numérica preestablecida que pueda hacerlo creer una precisa unidad de medida. En el lenguaje común, el término "dato" tiene, en cambio, una acepción más amplia, a menudo significando el conjunto de los contenidos registrados en la memoria de un computador, y por ser metafórico, también es utilizado para indicar el conjunto de las informaciones que representan. De otro lado, manifiesta que los *programas* o *softwares*, son constituidos,

[90] Véase MANTOVANI, Ferrando, *Diritto Penale, Parte Speciale*, Padova, Cedam, 2002, II, pp. 209 ss.

[91] Confróntese PECORELLA, Claudia, *art. 640 ter…*, número de margen 11.

[92] Por "datos", a estos efectos, se entienden aquellas representaciones de informaciones o conceptos que, siendo destinados a la elaboración por parte de un computador, son codificadas de forma electrónica, magnética, óptica o similares, no perceptibles visualmente (Véase PECORELLA, Claudia, "art. 635 bis", en DOLCINI, Emilio e MARINUCCI, Giorgio (a cura di), *Codice Penale Commentato*, Vicenza, Ipsoa, 2006, número de margen 12).

[93] Un "programa informático", a estos efectos, es aquel representado por un conjunto ordenado de instrucciones, a través de las cuales el computador sea capaz de obrar (Confróntese PECORELLA, Claudia, *art. 635 bis…*, número de margen 45).

[94] Ya que la información, entidad de por sí abstracta, es la que los datos expresan en forma codificada (así, PECORELLA, Claudia, *art. 635 bis…*, número de margen 15).

[95] Véase PECORELLA, Claudia, *art. 640 ter…*, número de margen 12.

[96] PICA, Giorgio, *op. cit.*, pp. 26 y 144.

en cambio, por una secuencia de instrucciones, constituidas, por lo tanto, de conjuntos de "datos" expresados en un lenguaje comprensible por la máquina, para que ella los elabore según lo planeado, y para que los ensamble para poder conseguirse de la máquina el cumplimiento de las operaciones preestablecidas, por simples o complejas que sean. Señala también que el término *software*, por lo tanto, aunque a veces resulta utilizado en la regla por contraste con *hardware*, es decir con los componentes físicos del computador que son visibles al ojo humano, indica, técnicamente, exclusivamente los programas que permiten al sistema funcionar y cumplir operaciones específicas, mientras, por otro lado, los contenidos informativos introducidos por el usuario se integrarían, técnicamente, en el concepto global de "datos". Por último, sostiene que la "información", entendida como contenido del sistema informático, es constituida, en cambio, por un conjunto más vasto de datos organizado según una lógica que permita atribuirles un particular sentido para el usuario de la máquina. En las normas penales, en cuyo tenor está presente la fórmula "datos, informaciones o programas", el legislador italiano –manifiesta el autor– no ha querido obrar un distingo técnico entre los múltiples conceptos, pero sí ha querido acoger omnicomprensivamente *cualquier* forma de dato registrado en los sistemas informáticos, cualquiera que sea su sentido intrínseco, para así evitar *lagunas* y vacíos de tutela que puedan derivar en una incompleta formulación conceptual. Entendida de esta forma, Pica estima que la amplitud de la primera modalidad comisiva de la *estafa informática* en su país (quien, alterando de cualquier modo el funcionamiento de un sistema informático o telemático), deja sin efecto alguno a la segunda (quien, interviniendo sin derecho de cualquier forma sobre los datos, informaciones o programas contenidos en un sistema informático o telemático o a ellos pertinente), puesto que, por definición, cuando se "altera el funcionamiento del sistema", siempre se influye en sus datos o programas, circunstancia que –en su opinión– determinará que dichos comportamientos representen únicamente una "especificidad ejecutiva" de la modalidad general; *interpretación* que le llevó a comprender que la única finalidad de haber establecido esta descripción, consistió en solventar cualquier posible duda sobre la idoneidad de ambas para dar lugar a la infracción penal, haciendo evidente, al mismo tiempo, que la intervención en los datos o *software* debería ser estimada como un acto preparatorio que finalmente sería absorbido por la consumación del delito en estudio. En contra de la última idea señalada, Antolisei[97] manifiesta que verdaderamente lo que persigue la segunda modalidad comisiva de este delito sería otorgar una adecuada cobertura a todas aquellas posibles y nuevas formas de abusos no contempladas por el legislador, cuya previsión se desbordaría con toda seguridad en el futuro.

Los datos, las informaciones y los programas tienen que ser "contenidos en un sistema informático o telemático o a ellos pertinente". Con base en la definición de "informaciones" explicada, se dice que debe descartarse que estas últimas puedan ser

[97] ANTOLISEI, Francesco, *op. cit.*, p. 375.

"contenidas" en un sistema informático. Así, a partir del momento de su introducción y memorización dentro del sistema, y hasta el momento de su emisión en forma perceptible por el ojo humano, las informaciones son representadas con el efecto de los "datos", en cuanto son codificados visualmente en una forma no perceptible[98].

Pueden considerarse "pertinentes" a un sistema informático las informaciones contenidas sobre soportes materiales, además de los datos y los programas contenidos sobre soportes externos al computador (como discos y cintas magnéticas u ópticas), que sean destinadas a ser utilizados en un sistema informático. Indiferente, al respecto, es la circunstancia de que se liberen datos o informaciones objeto de la primera elaboración, o bien, que sean procedentes de una elaboración ya producida. Lo que parece destacarse es únicamente la relación funcional que tiene que transcurrir entre el objeto de la manipulación (datos, informaciones o programas) y el proceso de elaboración que permita al agente procurarse una injusta ventaja económica con daño ajeno[99].

Existe una "intervención" sobre informaciones, datos o programas solamente cuando una acción produzca alguna modificación del contenido o de su destino. Tal intervención podrá considerarse "sin derecho" cada vez que sea ejecutada por quien no tenga facultad legítima al respecto y ha actuado de modo completamente arbitrario y, por lo tanto, injustificable. Este último requisito, en efecto, no parece tener una función diferente de la de llamar la atención del intérprete sobre el momento de la antijuridicidad[100].

Análogamente a la alteración del funcionamiento del sistema, también la intervención sin derecho sobre datos, informaciones y programas puede realizarse "con cualquier modalidad". Indiferente es, p. ej., que los datos sean borrados, o sustraídos a su elaboración, valiéndose de mandos del computador, o bien acercando un imán al soporte magnético sobre el que sea contenido[101].

La intervención sin derecho sobre informaciones destinadas a un tratamiento informático, y, por lo tanto, "pertinentes" a un sistema informático, constituye una de las posibles modalidades con las que se realizaría, indirectamente, una manipulación de *input*, en cuanto condiciona la calidad de los datos sucesivamente introducidos en el computador[102]. La segunda intervención puede consistir en la alteración, supresión o añadidura: sobre esta hipótesis, análoga a aquélla de introducción de datos falsos o

[98] Confróntese PECORELLA, Claudia, *art. 640 ter…*, número de margen 13.

[99] Véase PECORELLA, Claudia, *art. 640 ter…*, número de margen 14.

[100] Así, MANTOVANI, Ferrando, *op. cit.*, p. 210. En el mismo sentido, PICA, Giorgio, *op. cit.*, p. 146, pero éste dice que la presencia de este requisito sería completamente fuera de lugar, por tratarse de un delito relacionado con la consecución de un ilícito de acrecentamiento patrimonial, y, asimismo, señala que es peligroso, porque se prestaría a excluir la aplicabilidad del delito por el propio "*intranet*", que tiene el derecho a intervenir sobre los datos y sobre los programas.

[101] Atribuible a la hipótesis en examen es la modificación de los datos registrados en el computador sobre cuya base es efectuada el enlace a *Internet*, como resultado automático del enlace ocasional de parte de un usuario amateur a un servicio de tarifa aumentada, que implica una conexión a *Internet* por una diferente y más cara conexión (Véase PECORELLA, Claudia, *art. 640 ter…*, número de margen 16).

[102] Confróntese FANELLI, Andrea, *op. cit.*, pp. 415 ss.

de informaciones, se determinará la correspondiente interferencia sobre los datos que, sobre la base de aquellas informaciones, serán introducidos sucesivamente en el computador subordinado a un tratamiento informático. Cada intervención sobre las informaciones contribuiría, por lo tanto, inevitablemente, a la producción de un resultado inexacto del proceso de elaboración al que las informaciones mismas sean sometidas, después de haber sido convertidas en "datos"[103].

Una intervención no autorizada sobre los datos puede realizarse ya sea en la fase que precede la elaboración en sentido estricto, ya sea una vez acabada la elaboración, y se tratará, según los casos, de una manipulación de *input* o de *output*. Los datos manipulados podrán, indiferentemente, ser contenidos en el sistema informático –y eventualmente en la fase de transmisión de un sistema a otro– o bien, ser almacenados sobre un soporte externo, siempre que se trate de datos destinados a la elaboración. En todo caso, la manipulación tiene que ser capaz de provocar un resultado irregular del procedimiento de elaboración con respecto al que interviene[104].

La intervención sobre los datos podrá consistir tanto en una alteración o supresión de aquellos contenidos en el sistema o sobre un soporte externo, como en la introducción de datos falsos. Y el término "intervención" hace referencia a una acción que modifica, bajo un perfil funcional, algo ya existente. Por otro lado, en los casos –estadísticamente, además, más frecuentes– que sean insertados datos falsos en la memoria interior o externa de un computador, puede reconocerse una "intervención" sobre los datos ya presentes en el soporte de memoria, a los que los datos falsos vienen a sumarse[105].

Se ha manifestado que no puede reconocerse, en cambio, una *intervención sin derecho* sobre los datos, en el simple uso no autorizado de los datos integrantes del código personal de identificación ajena, con referencia a aquellos sistemas informáticos que permiten a un estrecho círculo de personas a ejecutar operaciones patrimonialmente relevantes, utilizando un terminal adecuado y un código personal de acceso. Es el caso, p. ej., más allá de los distribuidores automáticos de billetes, también, del servicio de "*home banking*", por el que los clientes de un banco pueden ejecutar una serie de operaciones bancarias –como contar con el dinero depositado sobre la propia cuenta por el pago de facturas, recibos y semejantes, o bien para efectuar un giro bancario sobre la cuenta ajena–, valiéndose de su terminal situado en casa y haciéndose reconocer el computador por los extremos del propio número de identificación. El *uso indebido* del código de identificación ajena, por otro lado, permite solamente el acceso al sistema informático, y puede evidenciar luego los objetivos del tipo de acceso abusivo a un sistema informático o telemático (art. 615 ter[106] del Código Penal italiano), y no también,

[103] Así, PECORELLA, Claudia, *art. 640 ter…*, número de margen 17.
[104] Véase PECORELLA, Claudia, *art. 640 ter…*, número de margen 18.
[105] Confróntese PECORELLA, Claudia, *art. 640 ter…*, número de margen 19.
[106] Esta norma prescribe: *"Quien, abusivamente se introduce en un sistema informático o telemático protegido por medidas de seguridad, o bien se mantiene en él contra la voluntad expresa o tácita de quien tiene el derecho a excluirlo, es castigado con pena privativa de libertad de hasta tres años. La pena es privativa de libertad de uno a cinco años: 1) si el hecho es cometido por un oficial público o un encargado de un público servicio, con abuso de los poderes o con violación*

de modo directo, la consecución de un injusto provecho. Este último, eventualmente, puede derivar del consiguiente cumplimiento –a través del computador– de un desplazamiento patrimonial injustificado, por una real "intervención sin derecho" sobre los datos, sobre la necesidad de que transcurra una relación consecuencial directa entre la conducta fraudulenta y la consecución de un injusto provecho con daño ajeno[107].

De otro lado, constituye una "intervención sin derecho"[108] sobre los datos contenidos en un sistema informático, la modificación de los datos relativos a la situación de la cuenta corriente sobre la que se reflejan las consecuencias de la operación económica realizada por quien ha conseguido abusivamente el acceso al sistema, utilizando el código de identificación ajeno. Se piensa, p. ej., en la modificación de tales datos con ocasión del cargo de sumas retiradas o trasladadas a otra cuenta. En caso de que, sin embargo, la operación económica se efectúe por medio del *uso abusivo de una tarjeta magnética de pago personal*, –sea ajena o falsa– será aplicable el art. 12[109] de la Ley 197/1991, que prevé, además, una pena más severa[110].

Una intervención sin derecho sobre los datos pertinentes a un sistema informático sería *reconocible* en la modificación de los datos registrados sobre la banda magnética de tarjetas de pago prepagadas, funcionales al empleo de aparatos automáticos que erogan bienes o servicios de pago, puestos a disposición de un círculo indeterminado de personas. En estos casos, la inserción de la tarjeta de pago, teniendo la misma función del dinero en efectivo, permitiría recibir directamente las prestaciones del aparato, sin pagar lo correspondientemente debido, y por lo tanto, de conseguirse un injusto provecho con daño ajeno se castiga en el sentido del art. 640 ter. La alteración de los datos contenidos sobre una tarjeta de pago "recargable" –como las de nueva introducción, funcionales para sufrir los riesgos de abuso a consecuencia de las operaciones comerciales efectuadas por *Internet*– se comprende, en cambio, dentro del ámbito de operatividad del art. 12 de la Ley 197/1991, en cuanto tales tarjetas, al ser "prepagadas", incluso

de los deberes inherentes a la función o al servicio, o también de quien ejerce abusivamente la profesión de investigador de vida privada, o con abuso de la calidad de operador del sistema; 2) si el culpable para cometer el hecho usa violencia sobre las cosas o en las personas, o bien si está abiertamente armado; 3) si del hecho deriva la destrucción o el perjuicio del sistema o la interrupción total o parcial de su funcionamiento, o bien la destrucción o el perjuicio de los datos, de las informaciones o de los programas en ellos contenidos. En caso de que los hechos de los incisos primero y segundo conciernan a sistemas informáticos o telemáticos de interés militar, o relativo al orden público o a la seguridad pública, o a la salud o a la protección civil, o en todo caso, de interés público, la pena es, respectivamente, privativa de libertad de uno a cinco años y de tres a ocho años. En el caso previsto por el primer inciso, el delito es punible a querella de la persona ofendida; en los otros casos se procede de oficio" (traducción del autor).

[107] Así, PECORELLA, Claudia, *art. 640 ter*…, número de margen 20.

[108] Véase PICA, Giorgio, *op. cit.*, pp. 146-147.

[109] Esta norma dispone, *"Tarjetas de crédito, de pago y documentos que habilitan el cobro de dinero en efectivo. Quien, para obtener provecho para sí o para otro, injustamente utiliza, no siendo el titular, tarjetas de crédito o de pago, o bien cualquier otro documento análogo que habilita al cobro de dinero en efectivo o a la adquisición de bienes o a la prestación de servicios, es castigado con pena privativa de libertad de uno a cinco años y con multa de seiscientos mil liras a tres millones de liras. A la misma pena se somete a quién, para obtener provecho para sí o para otro, falsifica o altera tarjetas de crédito o de pago o cualquier otro documento análogo que habilita al cobro de dinero en efectivo o a la adquisición de bienes o a la prestación de servicios, o bien posee, cede o adquiere tales papeles o documentos de procedencia ilícita, o en todo caso falsificados o alterados, además de la órdenes de pago producidas con ellos"* (traducción del autor).

[110] Así, PECORELLA, Claudia, *art. 640 ter*…, número de margen 21.

son nominativas[111].

Asimismo, una intervención sin derecho sobre el programa se integra por las *manipulaciones del programa*. Se trata, sin embargo, de hipótesis que ya tienen relevancia en el sentido del art. 640 ter, en cuanto determinan una "alteración del funcionamiento del sistema" en la que el programa sea utilizado. La superposición entre las dos previsiones consigue, por otro lado, la presencia en el tipo en examen de un ulterior elemento, no expresado por el legislador: la manipulación del programa –y más en general, la conducta fraudulenta– tiene que influir en el resultado de un proceso de elaboración, de modo que procure un injusto provecho con daño ajeno. Para tal fin se dice que es, por lo tanto, *necesario* que el programa manipulado sea utilizado en un sistema informático, provocando así una "alteración de su funcionamiento"[112].

Por otra parte, en el Derecho italiano se manifiesta que, a diferencia de la norma sobre la estafa tradicional, el delito de *estafa informática* del art. 640 ter no prevé expresamente un acontecimiento intermedio –en la estafa, el error– entre la conducta y los acontecimientos terminales provecho-daño, necesarios para la consumación del delito. En ausencia de tal elemento, se dice que la *estafa informática* conduciría a la idónea recomprensión de los hechos como "perjuicio informático", ya penalmente relevantes *ex* art. 635 bis[113] del Código Penal italiano, como hechos que violan completamente al patrimonio, como modalidad extraña a aquellas típicas del fraude[114].

2. Resultado típico: "resultado irregular del proceso de elaboración de datos que ha sido objeto de una interferencia indebida con daño ajeno"

Para asegurar a la norma en examen un *ámbito de operatividad* circunscrito, conforme a su *ratio*, el tipo debería ser enriquecido, en el plano interpretativo, de un *requisito tácito*[115], que localiza un nexo vinculado entre la conducta fraudulenta y la consecución del injusto provecho con daño ajeno y que refleja, al mismo tiempo, y de modo coherente, la realidad fenomenológica[116]. Parece, en otras palabras, *necesario* que el provecho injusto encuentre su fuente inmediata en el resultado irregular del proceso de elaboración que ha sido objeto de una interferencia indebida. De este modo, la *agresión* al patrimonio ajeno, que caracteriza a la *estafa informática*, viene a asumir un desarro-

[111] Véase PECORELLA, Claudia, *art. 640 ter…*, número de margen 22.

[112] Así, PECORELLA, Claudia, *art. 640 ter…*, número de margen 23.

[113] Esta norma dice, *"Perjuicio de sistemas informáticos y telemáticos. Quien, destruya deteriore o restituya, en todo o en parte, sistemas informáticos o telemáticos ajenos inservibles, o bien programas, informaciones o datos ajenos, son castigados, salvo que el hecho constituya un delito más grave, con pena privativa de libertad de seis meses a tres años. Si concurre una o más que las circunstancias del inciso segundo del artículo 635, o bien si el hecho es cometido con abuso de la calidad de operador del sistema, la pena es de privación de libertad de uno a cuatro años"* (traducción del autor).

[114] En este sentido, ANTOLISEI, Francesco, *op. cit.*, p. 374.

[115] De forma similar a lo que sucede con el elemento "acto de disposición" del delito de esta tradicional del art. 640 Código Penal italiano. Sobre esto, BALMACEDA HOYOS, Gustavo, *op. cit.*, pp. 223 y ss.

[116] Asimismo, al igual que en resultado típico del § 263a del Código Penal Alemán, en este lugar es válida en lo pertinente la explicación que dimos sobre la "disposición patrimonial perjudicial" del delito de estafa tradicional. Sobre esto, BALMACEDA HOYOS, Gustavo, *op. cit.*, pp. 223 y ss.

llo causal completamente simétrico que caracteriza ya a la estafa, y que ve como pasos lógicos *esenciales* a los siguientes[117]:

i) La alteración del funcionamiento del sistema informático, o bien la intervención sin derecho sobre datos, informaciones o programas;

ii) La modificación del resultado regular del proceso de elaboración; y,

iii) El provecho injusto con daño ajeno, como producto directo e inmediato del resultado alterado por el proceso de elaboración.

Finalmente, el resultado irregular del proceso de elaboración "manipulado" tiene que tener una *inmediata* consecuencia económica, y debe ser, por lo tanto, idóneo para incidir desfavorablemente en la esfera patrimonial ajena. Sólo por esta condición, en efecto, puede decirse que el daño que la víctima del fraude padece –como contrapartida del injusto provecho de otro que se ha conseguido– puede ser derivado directamente por los efectos desfavorables producidos en su esfera patrimonial del resultado alterado del procedimiento de elaboración[118].

V. EL MODELO DE "DEFINICIÓN GENERAL" DEL ART. 248.2 A) DEL CÓDIGO PENAL ESPAÑOL

1. Generalidades

Se debe manifestar que en España se efectúa una *tipificación amplia* o *general* de este delito, ya que no se establece una enumeración exhaustiva de sus modalidades comisivas. Así, el art. 248.2 a) del Código Penal español expresa que "*También se consideran reos de estafa: a) Los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro*"[119].

De la lectura de esta norma se desprende que la conducta típica de este delito consistirá en valerse de alguna manipulación informática o artificio semejante. Pongamos algunos *ejemplos* que se basan en supuestos de hecho reales que ha solucionado el TS:

[117] Así, PECORELLA, Claudia, *art. 640 ter…*, número de margen 26.
[118] Véase PECORELLA, Claudia, *art. 640 ter…*, número de margen 27.
[119] Dice el TS que esta conducta típica admite diferentes modalidades: desapoderar a otro de forma no consentida de su patrimonio, por medio de manipulaciones informáticas, bien del equipo, bien del programa, mediante la creación de órdenes de pago o de transferencias, ya sea a través de manipulaciones de entrada o salida de datos, en virtud de los cuales la máquina actúa en su función mecánica propia (por todas, confróntese STS 20/11/2001 [RJ, 2002, 805]; STS 26/06/2006 [RJ, 2006, 4925]).

i) Es un delito de *estafa informática* aquél en que el acusado aprovechó un fallo en el sistema informático de una entidad bancaria para obtener una importante cantidad de dinero, con las consecuencias por demás obvias de beneficiarse con ella en perjuicio de la primera. Y, en su opinión, el que esto hubiera respondido a un diseño de acción prefigurado con anterioridad o hubiera tenido lugar sobre la marcha y tras una primera comprobación ocasional, no añade ni quita nada al carácter típico de las correspondientes acciones[120];

ii) Sobre la utilización indebida de un terminal bancario de venta que estaba ubicado en una tienda abierta al público: el hijo de la dueña fue durante la madrugada a dicha tienda y dispuso de 52 millones de pesetas en su propio beneficio, aparentando diversas devoluciones de compras. Este hecho punible se cometió contra el patrimonio del Banco. Se manifestó que es claro que la propiedad del dinero es del Banco, porque los cuentacorrentistas lo ingresan en sus cuentas y, por lo tanto, al encontrarse en poder del Banco, forma parte del patrimonio de éste y no del de los titulares de las cuentas[121]; y,

iii) Sobre lo que deba entenderse por "artificio semejante", la jurisprudencia española ha dicho que la cuestión debe ser determinada por la aptitud del medio informático empleado para producir el daño patrimonial. En este sentido, dice que es equivalente, a los efectos del contenido de la ilicitud, que el autor modifique materialmente el programa informático indebidamente, o que lo utilice sin la debida autorización, o en forma contraria al deber[122].

Tenemos que dejar claro, desde ya, que en estos casos no se regulan las "estafas comunes cometidas en la red", sino que los supuestos de "estafas cometidas con manipulaciones informáticas"[123], es decir, aquellas "manipulaciones del proceso de elaboración electrónica de cualquier clase y en cualquier momento de éste, con la intención de obtener un beneficio económico, causando a un tercero un perjuicio patrimonial"[124], las cuales, sin ánimo de confusión, también pueden cometerse a través de *Internet* o de

[120] Véase STS 5/07/2004 (RJ 2004, 4182).
[121] Confróntese STS 21/12/2004 (RJ 2004, 8252).
[122] Véase STS 21/12/2004 (RJ 2004, 8252).
[123] CORCOY BIDASOLO, Mirentxu (et. al.), *Manual práctico de Derecho penal. Parte especial,* Valencia, Tirant lo Blanch, 2004, p. 588, da un ejemplo: subastas en *Internet* cuya foto de una cosa, una vez adjudicado el producto, no corresponde con el objeto ofrecido. En sentido similar, véase HILGENDORF, Eric, FRANK, Thomas y VALERIUS, Brian, *op. cit.*, número de margen 545, donde manifiestan que también la estafa tradicional, frente a un ser humano, ha obtenido nuevas formas de conducta por *Internet*. En ese sentido, sostienen que en muchos casos solo se trata de formas ya conocidas de la estafa, cambiando de aspecto, respecto a las cuales, no hay ninguna especialidad en el ámbito de la punibilidad. Así, agregan que en esos casos el autor solamente usa o abusa de las ventajas de *Internet*, pues es fácil de ocupar y, además, barata.
[124] Confróntese CORCOY BIDASOLO, Mirentxu y JOSHI JUBERT, Ujala, "Delitos contra el patrimonio cometidos por medios informáticos", en *Revista Jurídica de Cataluña*, 3, (1988), pp. 141 y ss.

cualquier tipo de red[125].

Ya entrando al estudio de la conducta típica del delito que nos ocupa, hay que decir que la referencia a dos posibles comportamientos alternativos lleva algunos autores[126] a estimar que, en principio, esta estructura típica respondería a los *tipos mixtos alternativos*, porque la posible acumulación de modalidades comisivas daría lugar a un delito único.

Ahora bien, nadie parece discutir que la hipótesis básica será la de *manipulación informática*, pero, sin embargo, no existe unanimidad en relación con su concepto, que ha sido criticado por ser estimado como confuso e indeterminado. Pero, no obstante finalmente es tolerado, debido a que gracias al desenfrenado desarrollo tecnológico, se dice que es necesario utilizar fórmulas de esta índole[127].

a) Conducta típica: "manipulación informática o artificio semejante"

En relación con esto, parece que la definición que ha encontrado una mejor acogida es la que en su día formuló Romeo Casabona[128], que la concibe como "…la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el computador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de tercero".

Este concepto parece *envolver*, en sus contornos fundamentales, todos los potenciales comportamientos efectuados en el ámbito de un sistema de tratamiento de datos que pudiesen ser nocivos para el patrimonio ajeno, atendiendo a las distintas etapas en que se pueda dividir un proceso de tratamiento informático de datos, es decir, el *input* o introducción de datos en el sistema[129], el tratamiento de dichos datos de acuerdo a las

[125] Así, ANARTE BORRALLO, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información", en *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, 1, (2001), p. 39; HERRERA MORENO, Myriam, "La estafa informática en el Derecho penal español", en *Actualidad penal*, 49, (2001), pp. 953 y ss.; GUTIÉRREZ FRANCÉS, Mª Luz, "Delincuencia económica e informática en el Nuevo Código Penal", en GALLARDO ORTIZ, Miguel Ángel (dir.), *Ámbito jurídico de las tecnologías de la información*, Madrid, CGPJ, 1996, p. 264.

[126] Véase GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 559.

[127] Véase ANARTE BORRALLO, Enrique, *op. cit.*, p. 42; BAJO FERNÁNDEZ, Miguel, *Los delitos de estafa en el Código Penal*, Madrid, Editorial Universitaria Ramón Areces, 2004, p. 166; GONZÁLEZ RUS, Juan José, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", en *Revista Electrónica de Ciencia Penal y Criminología*, 1, (1999), número de margen III.1. Disponible en: http://criminet.ugr.es/recpc/recpc_01-14.html. [Consulta: 03 noviembre 2011].

[128] Confróntese ROMEO CASABONA, Carlos María, *Poder informático y seguridad jurídica*, Madrid, Fundesco, 1988, p. 47. En el mismo sentido, por todos, confróntese MATA Y MARTÍN, Ricardo M., *Delincuencia informática y Derecho penal*, Madrid, Edisofer, 2001, p. 48; ORTS BERENGUER, Enrique y ROIG TORRES, Margarita, *Delitos informáticos y delitos comunes cometidos a través de la informática*, Valencia, Tirant lo Blanch, 2001, p. 64; PÉREZ MANZANO, Mercedes, "Las defraudaciones (I). Las Estafas", en BAJO FERNÁNDEZ, Miguel (dir.), *Compendio de Derecho penal. Parte especial*, Madrid, Editorial Centro de Estudios Ramón Areces, 1998, II, p. 455.

[129] Esta clase de comportamientos ha sido denominado como "amañado de datos", que es estimada como la manipulación informática por antonomasia, y que consiste en alterar, suprimir u ocultar datos antes o durante su introducción en el computador, lo que redundará en que esta clase de comportamientos en todo caso conlleven una

instrucciones del programa informático y el *output*, que constituiría la etapa de manifestación de los resultados en dicho proceso[130].

No obstante, otros autores reflexionan que las mencionadas manipulaciones en el "output" no podrían ser *discurridas* como comportamientos abarcables entre los constitutivos de los delitos que conformarían la "criminalidad informática", con lo que tampoco resultaría posible su inserción dentro de la propia noción de manipulación informática del delito examinado en el art. 248.2 a) del Código Penal español[131].

De cualquier manera, y aun frente a la posible precisión de esta conducta típica, parece que la *intención* del legislador español fue la de demarcarla de la forma más *amplia* posible, por medio del uso de expresiones como "alguna manipulación" o "valerse de", con el objeto de que en las mismas tengan cabida todos sus posibles cauces de ejecución (presentes o futuros)[132].

Por último, –como vimos– la *mayoría* de la doctrina española considera que existiría un paralelismo entre la "manipulación informática" y el "engaño" del delito de estafa, por medio del cual se intenta apoyar también un vínculo de cercanía o similitud entre la estructura típica de ambos injustos.

A pesar de la *amplitud* del concepto de "manipulación informática", en España se optó por contemplar una segunda modalidad comisiva –aquellos comportamientos que puedan estimarse como un "artificio semejante" que, por cierto, se trata de un elemento de *compleja* y debatida delimitación–, con el propósito de extender aún más esta conducta típica[133].

El legislador español pensó en esta voz para poder castigar también las manipulaciones en máquinas automáticas que proporcionan servicios o mercancías que en el caso concreto no pudieran calificarse como "informáticas", lo que es criticado, pues la obtención fraudulenta de este tipo de prestaciones probablemente nada tienen de

alteración del "input" (en este sentido, por todos, ORTS BERENGUER, Enrique y ROIG TORRES, Margarita, *op. cit.*, p. 64; ROVIRA DEL CANTO, Enrique, *op. cit.*, p. 271; HERRERA MORENO, Myriam, *op. cit.*, p. 936).

[130] Así, GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 561.

[131] Así, CORCOY BIDASOLO, Mirentxu y JOSHI JUBERT, Ujala, *op. cit.*, pp. 135-136 y 142, excluyen del ámbito típico de la estafa informática todos aquellos comportamientos que se efectúen mediante alteraciones realizadas fuera del sistema, es decir, de manera directamente asequible al conocimiento del ser humano. Dicho de otra manera, manifiestan que no se pueden calificar como estafas informáticas a aquellas manipulaciones de datos realizadas antes, durante o con posterioridad a la creación del programa, quedando los datos en forma accesible al ser humano. Además, debe subrayarse que en su concepto las estafas cometidas dentro del sistema se refieren a aquellas hipótesis en que los datos sean manipulados antes o durante la elaboración del programa, y afirman que se diferencian con las manipulaciones "fuera del sistema", en el hecho de que aquí la disposición patrimonial la efectúa la propia máquina. En el mismo sentido, VIVES ANTÓN, Tomás Salvador y GONZÁLEZ CUSSAC, José Luis, "Sección 1°, De las estafas", en VIVES ANTÓN, Tomás Salvador (coord.), *Comentarios al Código penal de 1995*, Valencia, Tirant lo Blanch, 1996, II, pp. 1237-1238. No obstante, esta interpretación –correctamente– ha sido rechaza por la doctrina. Confróntese, en este sentido, ROVIRA DEL CANTO, Enrique, *op. cit.*, pp. 573-574; ORTS BERENGUER, Enrique y ROIG TORRES, Margarita, *op. cit.*, p. 64; PÉREZ MANZANO, Mercedes, *op. cit.*, p. 455.

[132] Así, VALLE MUÑIZ, José Manuel y QUINTERO OLIVARES, Gonzalo, "Capítulo VI. De las defraudaciones", en *Comentarios a la Parte Especial del Derecho Penal*, QUINTERO OLIVARES, Gonzalo (dir.) y MORALES PRATS, Fermín (coord.), Pamplona, Aranzadi, 2007, p. 649.

[133] Así, GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 566.

semejante a una manipulación informática[134].

Para intentar solucionar este problema, algunos[135] definen la conducta típica de "manipulación informática" de forma *amplia*, pero respetuosa con la literalidad del concepto, considerándola como la "realización de todo tipo de operaciones que supusiesen un incorrecto uso o provocasen un incorrecto funcionamiento de un sistema de procesamiento de datos".

En virtud de este planteamiento se estimaría, por tanto, que el *sistema informático* afectado se trataría de un mero *instrumento* o medio de ejecución constitutivo de un *estafa informática*, postura que denota su rechazo –que no compartimos– frente a aquellas teorías que comparan el rol que cumple en este delito el sistema informático con el que efectúa la víctima del engaño en la *estafa informática*, pues se afirmaría que esto llevaría a "humanizar" a los computadores, atribuyéndole cualidades que nunca podrían poseer[136].

En fin, ante la *dificultad* de *delimitación* de ambas modalidades típicas, se ha llegado incluso a considerar factible una doble *interpretación*, es decir, como "artificio semejante a la manipulación"[137], o como "artificio semejante no informático"[138]; y en caso de calificarlo como informático –y esta es la interpretación "amplia" que seguimos en este trabajo–, creemos que es preferible estudiarlas de forma conjunta[139], pues con esta forma de describir el comportamiento típico lo que pretendería el legislador es cubrir todos los posibles procedimientos de uso irregular de un sistema informático[140].

A estos efectos, un concepto "amplio" evitaría el *casuismo*, permitiendo dar cabida a todas las posibles modalidades comisivas imaginables con salvaguarda de la seguridad

[134] Por todos, CHOCLÁN MONTALVO, José Antonio, "Estafa por computación y criminalidad económica vinculada a la informática", en *Actualidad penal*, 47, (1997), p. 1082.

[135] Confróntese GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 571, 583, 586 y 688. Asimismo, este autor –conforme a un criterio objetivo para configurar el vocablo "corrección"– considera que una interpretación coherente con el bien jurídico protegido debe atender a que sólo serán "manipulaciones informáticas" todos aquellos comportamientos –ejecutados en cualquiera de las fases del procesamiento de datos– que incidan o utilicen un sistema informático y que sean idóneos para producir una transferencia no consentida de activos patrimoniales. A mayor abundamiento, para el autor citado este tipo de conductas podrán ser consideradas como constitutivas de estafas informáticas siempre y cuando pudiesen determinar con su mera ejecución una verdadera y efectiva lesión patrimonial, es decir, siempre y cuando la alteración de los datos obtenida fuese por sí sola determinante de la existencia de un perjuicio patrimonial. El resto de manipulaciones –destinadas tan sólo a producir una falsa representación o apariencia respecto a la titularidad de los activos patrimoniales– resultarían en su opinión atípicas, aunque afirma que podrían adquirir relevancia penal en tanto se las considere como constitutivas de otros delitos, como una falsedad o una estafa tradicional.

[136] Así, GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 574, nota 953.

[137] Véase, por todos, GONZÁLEZ RUS, Juan José, *op. cit.*, número de margen III.1; BAJO FERNÁNDEZ, Miguel, *op. cit.*, p. 167; GUTIÉRREZ FRANCÉS, Mª Luz, *"Delincuencia económica"...*, p. 264.

[138] Esta es la interpretación restrictiva efectuada por VIVES ANTÓN, Tomás Salvador y GONZÁLEZ CUSSAC, José Luis, *op. cit.*, p. 1238, quienes estiman que la conducta típica debe incluir toda manipulación sobre ficheros o soportes informáticos. En sentido similar, MATA Y MARTÍN, Ricardo M., *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago: el uso fraudulento de tarjetas y otros instrumentos de pago*, Pamplona, Aranzadi, 2007, p. 93.

[139] Así, la jurisprudencia española. Por todas, véase STS 26/06/2006 (RJ 2006, 4925); SAP Madrid 3/03/2004 (JUR 2004, 260725); SAP Málaga 4/11/2002 (RJ 2003, 90990); STS 20/11/2001 (RJ, 2002, 805).

[140] En este sentido, por todos, VALLE MUÑIZ, José Manuel y QUINTERO OLIVARES, Gonzalo, *op. cit.*, p. 649.

jurídica y del principio de legalidad; y, por último, tendría la ventaja de no plantear dificultades a la hora de incardinar dentro de estas conductas a aquellas efectuadas por medio de un uso indebido del sistema implicado, resultando indiferente si se efectúa por quienes están autorizados a utilizar el sistema o por terceros ajenos al mismo[141].

De esta manera, algunos autores[142] –en una opinión que no creemos acertada– *rechazan* la utilización de la cláusula analógica (extensiva) que introduce la voz "artificio semejante" del art. 248.2 a) del Código Penal español, puesto que no ven qué conducta podría incardinarse en ella. Por ello, apuntan que la única interpretación que dotaría de *contenido material* a dicha cláusula sería aquella que la estima como una expresión que aluda a las denominadas manipulaciones semejantes "no informáticas", por lo que, en su concepto, esta modalidad típica debería referirse entonces a las conductas realizadas en aparatos y expendedores automáticos con funcionamiento completo o parcialmente *mecánico*, aunque advierten que su indeterminación generaría grandes problemas cuando haya que delimitarlas frente a las conductas en que el comportamiento típico también se caracterice por la realización de manipulaciones, alteraciones o simples usos no autorizados de aparatos automáticos –ya sea mecánicos o electrónicos– (de los arts. 283 –facturación falsa– y 255 –defraudaciones de fluido eléctrico y análogas– del Código Penal español), pero, afirman que, en cualquier caso, no parece que pueda determinarse la relación concursal que podría constatarse entre estos delitos atendiendo en forma exclusiva a las diferencias existentes entre sus conductas típicas.

b) Resultado típico: "transferencia no consentida de un activo patrimonial"

Por otro lado, el art. 248.2 a) del Código Penal español exige una "transferencia no consentida de activos patrimoniales", que debe ser un efecto inmediato de la manipulación informática[143], y vendría a representar el equivalente al "acto de disposición" de la estafa –si se mantiene un paralelismo estructural entre ambos delitos–.

[141] Confróntese GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 583 y 585.

[142] Asimismo, concluye a este respecto GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 586, 587, 588, 590 y 596-597, que como este tipo de conductas no son capaces de generar una transferencia de activos propiamente dicha, debería negarse su calificación como estafa informática, con lo que –a su juicio–, quedaría resuelta la polémica doctrinal y jurisprudencial existente. Por último, termina concluyendo que por este motivo tal cláusula pierde toda relevancia práctica, pues sólo sirve como punto de partida para la indeterminación de la conducta típica de este delito –lo que supondría, en su opinión, una infracción del principio de legalidad–, y porque la pretendida pretensión del legislador de cubrir todo tipo de "manipulación" quedaría cubierta ya por la voz "manipulación informática", razón por la que propone suprimir dicha cláusula analógica.

[143] Así, véase CHOCLÁN MONTALVO, José Antonio, "Estafa por computación"..., *op. cit.*, p. 1083 (a modo de resumen, este autor sostiene que, definido el efecto de la acción como "transferencia" resulta posible que sea realizada por una máquina sin intervención de una persona humana. De otro lado, afirma que la referencia a los "activos patrimoniales" tiene la clara finalidad de comprender como objeto de la acción el dinero contable o escritural, valores patrimoniales sin correspondencia con un objeto material. Por el contrario, sostiene que no pueden comprenderse en el precepto supuestos tales como la ocultación de bienes que constituya un alzamiento punible, en cuanto ello no es equivalente a una transferencia de un activo patrimonial, de modo que –en su concepto– en esos casos no es aplicable el art. 248.2 a) del Código Penal español aunque se esté en el caso de una manipulación informática que produce perjuicio a terceros).

Según algunos, esta exigencia típica parece cumplir la *función* de *resultado intermedio* en la *estafa informática*[144], caracterizándolo –al igual que en la estafa– como un hecho punible con un proceso causal que se encuentra típicamente configurado.

La "transferencia" constituye el efecto característico, material, la consecuencia directa de la acción[145]; y, jurídico-penalmente debe comprendérsela como el "cambio fáctico de adscripción patrimonial del elemento", del objeto material del resultado, y no puede quedar limitado su concepto a una "transferencia electrónica de fondos" o a una "transferencia bancaria de fondos"[146].

Asimismo, hay quienes señalan[147] –en una opinión que no compartimos, como veremos– que debe entenderse por "activos patrimoniales" aquellos que se encuentran *representados* mediante anotaciones informáticas que vendrán a incidir directamente sobre la titularidad de su valor patrimonial. Por tanto, su transferencia la conceptúan como una *transferencia electrónica* de activos meramente anotados o ideales. Esta consideración los lleva a *reducir* el ámbito de posibles servicios de ser transferidos –en el sentido del delito de *estafa informática*– a aquellos que pudiesen ser directamente prestados por el sistema informático manipulado, no pudiendo consistir en su concepto dicho uso en su mera reproducción, distribución o difusión pública no autorizada –porque en estos últimos casos entraría en juego un concurso de leyes que el autor aludido estima debería resolverse conforme al principio de especialidad–. Con esta postura, se inclinan por la denominada "concepción estricta" de la transferencia de activos, porque –en su opinión– la exigencia de que el traspaso se derivase directamente de la manipulación sólo se podrá cumplir cuando los datos sobre los que recaiga tengan trascendencia patrimonial por sí mismos[148].

En este sentido, para algunos[149] una *correcta delimitación* de los activos patrimoniales que sean susceptibles de ser objeto material del delito de *estafa informática* llevará consigo la *exigencia* de una estricta unión entre el valor económico patrimonial que se lesiona con la consumación de este delito y los registros informáticos que se alteran con su realización. Así, consideran que sólo aquellas alteraciones que recaigan sobre *registros informáticos* susceptibles de tener en forma *directa* una importancia patrimonial efectiva –material–, podrían ser estimadas como constitutivas de un delito de *estafa informática*, quedando por ello el resto de hipótesis fuera, pudiendo ser constitutivas de otros delitos contra el patrimonio –como una estafa– o, incluso, de otros delitos protectores de bienes jurídicos no patrimoniales –como las falsedades–. De esta manera, entienden que a efectos de este delito serán *activos* patrimoniales aquellos que "estando representados mediante anotaciones o registros informáticos, queden adscritos de tal forma a

[144] Por todos, GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 591.
[145] Así, ROVIRA DEL CANTO, Enrique, *op. cit.*, p. 584.
[146] En el mismo sentido, PÉREZ MANZANO, Mercedes, *op. cit.*, p. 456.
[147] Así, GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 605, 607 y 609.
[148] Así, GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 600.
[149] Así, GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 604, 609, 610 y 612-613.

éstos, que su cambio o alteración, podría provocar la traslación del valor económico que representan a un tercero, con la consiguiente pérdida de la capacidad de disposición sobre los mismos, de la que gozaba su titular inicial; pérdida que en todo caso deberá ser efectiva y real, y no meramente posible, aparente o formal". Atendiendo a estas exigencias, frente a un sinnúmero de servicios que son prestados en línea (*online*), la obtención de los mismos en forma fraudulenta no representan en su opinión una hipótesis de *estafa informática*, sino que un mero uso no autorizado de sistemas informáticos ajenos y de los servicios que los mismos podrían brindar, de naturaleza cercana a lo que tradicionalmente se denomina "hurto de uso" (usos no apropiatorios de bienes o de servicios ajenos), –que se han venido considerando *atípicos*, salvo previsión expresa en contrario–, ya que a su entender la consumación de este delito no se derivaría de la transferencia de activos efectuada, sino del impago del crédito que surgiría como consecuencia del servicio prestado –como sucede con los servicios de detección y supresión de virus, emisión de prepago de películas o música, postales electrónicas, etc.–.

Por *nuestra parte* –siguiendo a Pérez Manzano[150]–, nos inclinamos por una *interpretación amplia* de "activo patrimonial", *sosteniendo que sus elementos se componen por todos aquellos bienes o derechos que tienen una valoración económica positiva; considerando lo que es activo o pasivo no como cualidad inherente al objeto, sino como dependiente del titular del patrimonio*. Desde este punto de vista, p. ej., si el deudor transfiere una deuda a un tercero, está transfiriendo un activo patrimonial del acreedor en perjuicio de un tercero.

En todo caso, no es suficiente para la apreciación del delito de *estafa informática* con la *constatación* de una transferencia de activos patrimoniales como resultado de una manipulación informática, sino que el tipo de este delito exige que la transferencia aludida se efectúe de forma "no consentida"[151].

Esta característica será la que vendría a posibilitar –según algunos[152]– que se pudiese equiparar la "transferencia no consentida de activos patrimoniales" al "error" del disponente del delito de estafa.

La postura que mantiene la *mayoría* de la doctrina española con respecto al *consentimiento* es que éste delimita el tipo de los delitos patrimoniales, y no constituye entonces una causa de justificación, ya que su concurrencia conllevaría la irrelevancia típica del comportamiento llevado a cabo (dado el carácter disponible del bien jurídico protegido)[153].

Esta consideración del *rol* que desempeñaría el consentimiento podría hacer parecer como redundante la exigencia típica de su "ausencia", pero, sin embargo, ello no es así,

[150] PÉREZ MANZANO, Mercedes, *op. cit.*, pp. 456-457. En el mismo sentido, BAJO FERNÁNDEZ, Miguel, *op. cit.*, p. 167.

[151] Confróntese GALÁN MUÑOZ, Alfonso, *El fraude*..., *op. cit.*, pp. 616 y ss.

[152] Véase, por todos, PÉREZ MANZANO, Mercedes, *op. cit.*, p. 456.

[153] Confróntese, por todos, PÉREZ MANZANO, Mercedes, *op. cit.*, p. 456. De otra opinión, CONDE-PUMPIDO FERREIRO, Cándido, *Estafas*, Valencia, Tirant lo Blanch, 1997, pp. 222-223.

ya que este elemento no se refiere a la producción del perjuicio patrimonial –resultado del delito–, sino que al hecho de que es "suficiente" con que se consintiese la transferencia patrimonial para que la conducta fuese excluida del art. 248.2 a) del Código Penal español[154].

Esta tesis sobre la *naturaleza del consentimiento* tiene grandes efectos al momento de concretar los elementos que tiene que reunir, *requisitos* que se pueden agrupar en *subjetivos* y *objetivos*. Los primeros son aquellos que aluden a las cualidades que debe agrupar el sujeto emisor del consentimiento –por ello, los elementos subjetivos se refieren a la "legitimación" y "capacidad" del sujeto– (entonces, sirven para concretar quién se encuentra facultado para brindarlo). Los requisitos objetivos, en cambio, hacen referencia a las exigencias que debe reunir la expresión de voluntad para ser idónea en la exclusión de la tipicidad (esto es, dicen relación con el "momento" en que se emite, con su "contenido" y, por último, con su "validez")[155]. En seguida, estudiaremos uno a uno[156].

Con respecto a la "legitimación", podemos decir que el sujeto legitimado no siempre deberá ser el titular o propietario de los activos patrimoniales que se transfieren (porque el consentimiento excluyente de la tipicidad no tiene que relacionarse con la producción del perjuicio patrimonial). De este modo, será la efectiva capacidad de disposición o de transferencia temporal de quien consiente la que toleraría *delimitar* el injusto del delito de *estafa informática* con respecto a otros delitos, como el de estafa o el de apropiación indebida.

De otro lado, la "capacidad jurídica" que debe tener el emisor del consentimiento será viable aún si se emite sin cumplir con todos los requisitos civilmente exigibles, ya que se trataría de una causal de exclusión del tipo, y no de justificación (caso en el que sí deberían exigirse, atendiendo a la unidad del Ordenamiento jurídico en sede de antijuridicidad), resultando penalmente válida aquella capacidad de percibir en lo esencial la trascendencia del acto que ejecuta, puesto que nadie puede querer, ni por tanto consentir, aquello que no conoce y no comprende.

En cuanto al "momento" en que deba prestarse, parece indiscutible que debe otorgarse con anterioridad o, al menos, simultáneamente a la producción de la transferencia patrimonial; y, en relación con el "contenido", el consentimiento debería decir relación con la transferencia propiamente tal, con el activo patrimonial transferido, y con la persona en cuyo favor se realiza. Por último, la "validez" del consentimiento se vincula con la inexistencia de vicios de la voluntad del emisor.

En otro orden de ideas, algún autor[157] afirma que el tenor literal del art. 248.2 a) del Código Penal español solamente exige una "ausencia de consentimiento", sin ninguna

[154] Véase GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 618-619. Asimismo, este autor apunta que la presencia del consentimiento se presenta como un criterio básico para el establecimiento de sus contornos con respecto al de otros delitos contra el patrimonio, como la estafa genérica o la apropiación indebida, caracterizados por el hecho de que la merma patrimonial se genera como consecuencia de un traspaso voluntario.

[155] Véase GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 621 ss.

[156] Confróntese GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 621, 624, 628, 630, y 633-634.

[157] Así, GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 634.

otra referencia adicional, exigencia que parece manifestar la inexigibilidad de que el emisor señale "expresamente" una voluntad contraria a la misma, ya que, –en su concepto– de requerirse una manifestación expresa en tal sentido, "se hubiese exigido en sede de tipicidad que la transferencia obtenida fuese realizada contra su voluntad y no simplemente sin su consentimiento".

Sobre el particular, el autor referido[158] sostiene que no puede *olvidarse* que lo que debería probarse positivamente es la "ausencia del consentimiento", no resultando suficiente la afirmación de la imposibilidad de constatar su presencia –en forma expresa, tácita o incluso presunta–, ya que ello llevaría a establecer una presunción *iuris tantum* al respecto, lo que sería contrario al principio de presunción de inocencia, que asimismo obligaría a que en las hipótesis de duda sobre la existencia o no del mismo debiese optarse por la absolución. Así, en cuanto a su prueba, sostiene este autor que si de la valoración de las mismas no se puede inferir la ausencia del consentimiento, el comportamiento debería considerarse como atípico, pero no sobre la base de un "inexistente", y en todo caso "dudosamente presumible consentimiento", sino por la carencia de prueba sobre su ausencia.

Recapitulando lo dicho hasta el momento, *el consentimiento, entendido como "voluntad conforme a la realización de la transferencia de activos" para que pueda determinar la exclusión de la tipicidad, no será suficiente con la creencia del autor respecto a su existencia, sino que deberá haber sido verdaderamente manifestada al exterior, pudiendo manifestarse tanto de forma expresa como por medio de actos concluyentes*[159].

Así las cosas, quienes consideran la transferencia no consentida de activos patrimoniales como *resultado intermedio* del delito de *estafa informática*[160], unido a las exigencias básicas de la relación de causalidad e imputación objetiva que debería unirla con la conducta típica de este delito, todo esto determinaría que venga a ser el "referente" fundamental cuando tengan que delimitarse las manipulaciones informáticas relevantes a efectos de este delito, función análoga a la que cumpliría el "error" con respecto a la conducta del delito de estafa –si se le considera a éste como resultado intermedio del delito de estafa tradicional–.

De esta manera, y de acuerdo con la definición que Galán Muñoz[161] sostiene de "manipulación informática", –que no compartimos del todo[162]– manifiesta que para

[158] GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 644 y 646.

[159] Véase GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 647, y 348-350.

[160] Así, GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 649-650, quien considera, por tanto, que la idoneidad del comportamiento efectuado para obtener una transferencia no consentida de activos patrimoniales ajenos pasaría a transformarse en el referente básico del desvalor de acción del delito del art. 248.2 a) del Código Penal español, viniendo la alusión típica a la manipulación informática simplemente a determinar la herramienta por medio de la que se debería obtener dicho resultado típico. Comprendida de esta forma la conducta típica de este delito, se estimaría de una forma tan amplia, que no parecería presentar obstáculos para la apreciación de su comisión por omisión, ya que no habría un comportamiento "determinado", como sucedería –en opinión de este autor– en el delito de estafa genérica.

[161] GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 653.

[162] Aclaramos esto, porque compartimos su opinión de que es viable una estafa informática en comisión por omisión, pero no estamos de acuerdo con su planteamiento inicial. A favor de esto, véase CRAMER, Peter y

que un sujeto pueda estimarse como autor de una *estafa informática* en comisión por omisión debería encontrarse en una posición de garante, pero no con respecto al funcionamiento o al resultado del proceso realizado por el sistema informático, sino con respecto a la generación del perjuicio patrimonial derivado de la transferencia informática de activos patrimoniales ajenos.

Teniendo esto presente, el autor aludido[163] *concluye* que no toda vinculación laboral o contractual podría servir de fundamento para la constatación de un vínculo especial del presunto autor con respecto al patrimonio de terceros. En este contexto, entiende que sólo podrá apreciarse una asunción voluntaria de funciones de protección del bien jurídico en aquellos contratos en los que el sujeto ostentase –como consecuencia de su perfección– un especial *deber de lealtad o fidelidad* con respecto al patrimonio del tercero. Por último, afirma que estos sujetos, al igual que todos aquellos que no se encontrasen en la *posición de garante* indicada, sólo podrán adquirir un especial deber de evitar el resultado típico cuando con su actuación precedente los hubieran puesto en peligro –idea de injerencia–, pero siempre que la creación o el incremento del riesgo no se derivase de su propia y previa actuación dolosa. Así, nuestro autor señala que nos podríamos encontrar con los casos de quien pudo evitar el resultado y no lo hizo, pese a haber asumido –previa y voluntariamente– funciones de protección del bien jurídico. También, junto a ellos, sostiene que podría plantearse la viabilidad de comisión omisiva por injerencia cuando el fundamento de la posición de garante no se derive de su actuar doloso previo, sino de un comportamiento activo previo e imprudente. Sin embargo, termina por rechazar esta última hipótesis, pues afirma que en su realización no concurre la presencia de la intención de obtener un beneficio patrimonial propio o de terceros –como se exige en el tipo de este delito–. De esta manera, –y aquí se encuentra la base de la diferencia de opinión que tenemos con este autor– Galán Muñoz[164] apunta que resulta totalmente *inviable* la *apreciación* de la comisión por omisión de un delito de *estafa informática* sobre la base de la realización previa de una conducta de injerencia del omitente, con lo que concluye que finalmente debería excluirse toda hipótesis de comisión omisiva de dicho delito, postura que, sin embargo, no quiere significar que toda omisión sería irrelevante a efectos del art. 248.2 a) del Código Penal español, pues sostiene que resulta perfectamente viable constatar la participación omisiva en este delito.

VI. CONCLUSIONES

i) El injusto del delito de "estafa informática" no sólo presentaría una estrecha proximidad con el delito de estafa clásico. A nuestro entender, parece razonable efectuar

PERRON, Walter, *op. cit.*, número de margen 4; KINDHÄUSER, Urs, *op. cit.*, número de margen 15.

[163] Confróntese GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, p. 653.

[164] GALÁN MUÑOZ, Alfonso, *El fraude...*, *op. cit.*, pp. 654-655 y 660-661.

una lectura alternativa del tipo de estafa clásico con el fin de posibilitar la inclusión en su seno de las conductas que se contemplan en la estafa informática (con todas las lógicas consecuencias que de ello se derivan).

ii) Así, podemos afirmar que su expresa tipificación solamente establecería una interpretación auténtica de los límites del injusto del delito de estafa tradicional.

iii) En este sentido, lo que constituya engaño deberá configurarse por medio de la "interpretación", teniéndose presente algo que estimamos se olvida con frecuencia: en la interpretación no sólo debería tenerse presente el antecedente histórico del precepto, sino que también la "realidad social" de la época en que corresponda su aplicación, lo que no significaría, en nuestra opinión, violentar el principio de legalidad.

iv) Resulta obvio que no se engaña a una máquina, la que, simplemente, constituye un instrumento al servicio del hombre. De esta manera, en la "estafa informática" el computador nunca aparece como receptor de un engaño ni sufre un error, ya que la máquina opera siempre correctamente y conforme con los datos o instrucciones que le den.

v) Por estas razones, en aquellos casos en que intervenga un ser humano, también aquí debería entenderse que quien resulta finalmente engañado es, en realidad, el titular del patrimonio afectado.

vi) Entonces, sería más acorde con nuestra propuesta señalar que el engaño no constituiría un problema para encajar a la "estafa informática" dentro de la estafa, pues no sería consustancial al concepto de engaño que tenga como receptor a una persona física, bastando con que el falseamiento intencional de la realidad que el engaño implica se exteriorice, o sea, que no se quede en la esfera interna del individuo, de la misma manera que se puede engañar a una o varias personas, físicas o jurídicas, directa o indirectamente.

vii) Para poder determinar la idoneidad de las manipulaciones informáticas para producir error en otro, se ha estimado preferible desterrar la idea "psicológica" del error, procedente de un modelo de relaciones negociales que ha evolucionado notablemente.

viii) Nos parece que se tiene que examinar la operatividad e idoneidad del engaño, atendiendo a las "concretas" circunstancias de la víctima, descargando de importancia el tema de la posible "vencibilidad" del error, o de las medidas que se tomen para defenderse del engaño (salvo, claro está, aunque no de forma rotunda, en los

casos de manipulaciones informáticas producidas en Internet, cuando la víctima haya sido "totalmente" negligente en sus deberes de autoprotección –porque en aquellos casos en que la manipulación sea objetivamente idónea para poder producir la transferencia no consentida de un activo patrimonial, consideramos que el deber de autoprotección es mínimo–).

ix) Según se ha manifestado, en el Derecho europeo continental los sistemas legislativos que dicen relación con la "estafa informática" son diferentes. Así, hay que distinguir entre aquellos países que efectúan una descripción "exhaustiva" (e incluso, enumerativa) de las conductas típicas (como sucede en Alemania o Portugal); y, entre aquellos países que utilizan "definiciones generales" (como acontece en Italia y España).

x) Sea cual sea el modelo adoptado, parece inexacto un esfuerzo que detalle todas las maneras posibles de manipulación de elementos informáticos a través de un listado completo y acabado. No obstante, creemos que antes de poderse efectuar una elaboración jurídica respecto al tema, deberían tenerse presente los conceptos técnicos fundamentales que dicen relación con el problema.

xi) Como principio general, el legislador comparado ha descrito como conducta típica del delito de "estafa informática" a la "manipulación informática", concepto que ha sido objeto de polémica.

xii) De *lege lata*, y aun frente a la posible precisión de esta conducta típica, la intención del legislador comparado fue la de demarcarla de la forma más amplia posible, por medio del uso de expresiones, p. ej., como hace el legislador español, de "alguna manipulación" o "valerse de", con el objeto de que en las mismas tengan cabida todos sus posibles cauces de ejecución (presentes o futuros).

xiii) Por último, la mayoría de la doctrina comparada considera que existiría un paralelismo estructural entre la "manipulación informática" y el "engaño" del delito de estafa, por medio del cual se intenta apoyar también un vínculo de cercanía o similitud entre la estructura típica de ambos injustos.

[Recibido el 3 de noviembre y aceptado el 3 de diciembre de 2011]

BIBLIOGRAFÍA

ANTOLISEI, Francesco, *Manuale di Diritto Penale, Parte speciale*, a cura di Luigi Conti, Milano, Multa Pavcis, 2002, I.

ANARTE BORRALLO, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho penal en la sociedad de la información", en *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, 1, (2001).

ARZT, Gunther y WEBER, Ulrich, *Strafrecht, Besonderer Teil*, Bielefeld, Verlag Ernst und Werner Gieseking, 2000.

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

BALMACEDA HOYOS, Gustavo, *El delito de estafa informática*, Santiago, Ediciones Jurídicas de Santiago, 2009.

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

CORCOY BIDASOLO, Mirentxu (et. al.), *Manual práctico de Derecho penal. Parte especial*, Valencia, Tirant lo Blanch, 2004.

CORCOY BIDASOLO, Mirentxu y JOSHI JUBERT, Ujala, "Delitos contra el patrimonio cometidos por medios informáticos", en *Revista Jurídica de Cataluña*, 3, (1988).

CRAMER, Peter y PERRON, Walter, "§ 263a", en SCHÖNKE Adolf, SCHRÖDER Horst y CRAMER Peter (eds.), *Strafgesetzbuch Kommentar*, München, C.H. Beck, 2006.

FANELLI, Andrea, *La truffa*, Milano, Giuffrè, 1998.

FIANDACA, Giovanni, MUSCO, Enzo, *Diritto penale, Parte speciale, I delitti contro il patrimonio*, Bologna, Zanichelli editore, 2005, vol. II, II.

FISCHER, Thomas, *Strafgesetzbuch und Nebengezetse*, München, C.H. Beck, 2008.

GONZÁLEZ RUS, Juan José, "Protección penal de sistemas, elementos, datos, documentos y programas informáticos", en *Revista Electrónica de Ciencia Penal y Criminología*, 1, (1999). Disponible en: http://criminet.ugr.es/recpc/recpc_01-14.html. [Consulta: 03 noviembre 2011].

GUTIÉRREZ FRANCÉS, Mª Luz, *Fraude informático y estafa*, Madrid, Ministerio de Justicia, 1991.

_____. "Delincuencia económica e informática en el Nuevo Código Penal", en GALLARDO ORTIZ, Miguel Ángel (dir.), *Ámbito jurídico de las tecnologías de la información*, Madrid, CGPJ, 1996.

HERRERA MORENO, Myriam, "La estafa informática en el Derecho penal español", en *Actualidad penal*, 49, (2001).

HILGENDORF, Eric, FRANK, Thomas y VALERIUS, Brian, *Computer- und Internetstrafrecht*, Berlin, Springer, 2005.

HOYER, Andreas, "§ 263a", en *Systematischer Kommentar zum Strafgesetzbuch*, Band II, BT (§§ 80 - 358), Neuwied, Luchterhand, 2006.

KINDHÄUSER, Urs, "§ 263a", en *Nomos Kommentar zum Strafgesetzbuch*, Nomos, Baden Baden, 2005.

LACKNER, Karl, "Zum Stellenwert der Gesetzestechnik. Dargestellt an einem Beispiel aus dem Zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität", en AAVV, *Festschrift für Herbert Tröndle*, Berlin - New York, Walter de Gruyter, 1989.

LACKNER, Karl y KÜHL, Kristian, "§ 263a", en *Strafgesetzbuch Kommentar*, München, C.H. Beck, 2007.

MANTOVANI, Ferrando, *Diritto Penale, Parte Speciale*, Padova, Cedam, 2002, II.

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

_____. *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago: el uso fraudulento de tarjetas y otros instrumentos de pago,* Pamplona, Aranzadi, 2007.

MAURACH, Reinhart, SCHROEDER, Friedrich-Christian y MAIWALD, Manfred, *Strafrecht, Besonderer Teil, Teilband 1*, Heildelberg, C.F. Müller Verlag, 2003.

MITSCH, Wolfgang, *Strafrecht. Besonderer Teil 2, Teilband 2*, Berlin, Springer, 2001.

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

PECORELLA, Claudia, "art. 635 bis", en DOLCINI, Emilio e MARINUCCI, Giorgio (a cura di), *Codice Penale Commentato*, Vicenza, Ipsoa, 2006.

_____. "art. 640 ter", en DOLCINI, Emilio e MARINUCCI, Giorgio (a cura di), *Codice Penale Commentato*, Vicenza, Ipsoa, 2006.

PÉREZ MANZANO, Mercedes, "Las defraudaciones (I). Las Estafas", en BAJO FERNÁNDEZ, Miguel (dir.), *Compendio de Derecho penal. Parte especial,* Madrid, Editorial Centro de Estudios Ramón Areces, 1998, II.

PICA, Giorgio, *Diritto penale delle tecnologie informatiche*, Turín, Utet, 1999.

PIOLETTI, Ugo, voz "Truffa", en *Novissimo Digesto Italiano*, 1987.

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

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

SIEBER, Ulrich, *Computerkriminalität und Strafrecht*, Köln - Berlin - Bonn - München, Carl Heymanns Verlag KG, 1980.

_____. *Informationstechnologie und Strafrechtsreform*, Köln - Berlin - Bonn - München, Carl Heymanns Verlag KG, 1985.

TIEDEMANN, Klaus, "§ 263a", en *Leipziger Kommentar zum Strafgesetzbuch*, Berlin, De Gruyter Recht, 1997, VI.

_____. *Wirtschaftsstrafrecht. Besonderer Teil mit wichtigen Gesetzes- und Verordnungstexten*, München, Carl Heymanns Verlag, 2008.

VALLE MUÑIZ, José Manuel y QUINTERO OLIVARES, Gonzalo, "Capítulo VI. De las defraudaciones", en QUINTERO OLIVARES, Gonzalo (dir.) y MORALES PRATS, Fermín (coord.), *Comentarios a la Parte Especial del Derecho Penal*, Pamplona, Aranzadi, 2007.

VIVES ANTÓN, Tomás Salvador y GONZÁLEZ CUSSAC, José Luis, "Sección 1°, De las estafas", en VIVES ANTÓN, Tomás Salvador (coord.), *Comentarios al Código penal de 1995*, Valencia, Tirant lo Blanch, 1996, II.

WESSELS, Johannes y HILLENKAMP, Thomas, *Strafrecht, Besonderer Teil/2*, Heildelberg, C.F. Müller Verlag, 2007.

ZAHN, Gesche, *Die Betrugsähnlichkeit des Computerbetrugs (§ 263a StGB)*, Aechen, Shaker Verlag, 2000.