UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

CONSTRUCCIÓN LEGISLATIVA Y APLICACIÓN JURISPRUDENCIAL DEL DELITO DE “ESTAFA” INFORMÁTICA EN COSTA RICA DEL AÑO 2014 AL 2019. ÉNFASIS EN EL USO INDEBIDO DE DATOS.

Trabajo final de investigación aplicada sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Derecho para optar al grado y título de Maestría Profesional en Ciencias Penales.

FREDDY CALDERÓN CHAVES

Ciudad Universitaria Rodrigo Facio, Costa Rica

2021.

Dedicatoria

A mi novia feminista y brillante jurista, Laura Cervantes Ocampo.

A mi hija Fiorella, para quien deseo que nunca deje de buscar el conocimiento.

Agradecimientos

A Laura, por sus valiosos aportes.

A mi mamá Cecilia, por incentivarme a estudiar.

A mi profesor, Erick Gatgens, por el tiempo dedicado a esta investigación.

"Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Derecho de la Universidad de Costa Rica, como requisito parcial para optar por el grado y título de Maestría Profesional en Ciencias Penales."

Dr. Rafael González Ballar
Representante del Decano
Sistema de Estudios de Posgrado

Dr. Erick Gatgens Gómez
Profesor Guía

Dr. Eric Alfredo Chirino Sánchez
Lector

MSc. Sergio Múnera Chavarría
Lector

MSc. Mauricio París Cruz
Representante Programa de Posgrado en Derecho

Freddy Calderón Chaves
Sustentante

Tabla de contenido

Dedicatoria ii

Agradecimientos iii

Hoja de aprobación iv

Tabla de contenido v

Resumen vii

Índice de tablas viii

Índice de gráficos ix

Lista de abreviaturas x

Introducción 1

Capítulo I. Tratamiento de la estafa informática a nivel doctrinal 12

Capítulo II. Comparación entre estafa general y estafa informática 30

Estafa general 31

Estafa informática 36

Verbos típicos de la estafa informática 46

Uso de datos falsos, incompletos, indebidos o de programación. Valerse de operación informática o artificio tecnológico 46

Manipular 48

Influir 57

Incidir 58

Dosificación penal de la estafa informática en comparación con la estafa convencional 61

Bien jurídico tutelado de la estafa informática 70

Derecho comparado 101

Alemania 101

Argentina 104

España 106

Capítulo III. Fundamentos legislativos para la construcción del tipo penal de estafa informática..... 111

Discusión legislativa..... 115

Capítulo IV. Tratamiento jurisprudencial de la estafa informática en Costa Rica durante los años 2014 al 2019 149

Resoluciones de STCSJ del año 2012 al 2019..... 150

Resoluciones del TASPIICJSJ del 2014 al 2019 161

Conclusiones..... 203

Bibliografía 215

Resumen

La presente investigación, aborda el delito de “estafa” informática previsto en el artículo 217 bis del Código Penal, desde diversas perspectivas de investigación. Iniciando en el primer capítulo, con su matiz de delincuencia no convencional, por ser un tipo penal al cual le antecede una ciencia novedosa para el mundo del derecho, tal y como lo es la informática. Asimismo, el contexto social y mundial en el que nos desenvolvemos, propicia que la informática sea una herramienta indispensable en nuestro diario vivir, siendo insoslayable que, en ocasiones se hace un uso indebido de ella, con la intención de perjudicar a otras personas.

En razón de lo anterior y atendiendo la redacción del artículo 217 bis del Código Penal, en el segundo capítulo, se llevó a cabo una comparación con la estafa general del numeral 216 del mismo cuerpo normativo, con la intención de delimitar, si la estafa informática es una verdadera estafa o si prevé supuestos fácticos distintos de punición. También, se aborda la dosimetría penal establecida en los *supra* indicados tipos penales, para visibilizar no sólo las diferencias abismales que existen en ellos, sino, además, cuáles son las razones para que ello sea así. No se deja de lado un estudio de derecho comparado con los países de Alemania, Argentina y España.

Las discusiones legislativas de mayor trascendencia al momento de aprobar la actual redacción del artículo 217 bis del Código Penal, serán reflejadas en el tercer capítulo y de esa manera delimitar si quienes legislaron se apoyaron en datos duros y científicos para construir un tipo penal útil en resguardo de las víctimas de esta delincuencia y teniendo una visión de prevención especial positiva de la pena para quien delinque.

El enfoque jurisprudencial resulta trascendente y es expuesto en el último de los capítulos, tomando en cuenta resoluciones judiciales de la Sala Tercera de la Corte Suprema de Justicia y del Tribunal de Apelación de Sentencia Penal del II Circuito Judicial de San José, durante los años del 2014 hasta el 2019; lapso amplio que, desde un enfoque cualitativo, nos permitirá arribar a conclusiones que se espera sean relevantes para eventuales reformas legislativas, en pro de las personas que son usuarias de los procesos penales.

Índice de tablas

Tabla 1. Connotaciones de la criminalidad por computadora 25

Tabla 2. Diferencias entre la estafa general y la estafa informática 39

Tabla 3. Dosimetría penal entre estafa general y estafa informática 62

Tabla 4. Agravantes de pena en estafa general y estafa informática 65

Tabla 5. Principios de la autodeterminación informativa 79

Tabla 6. Comparación entre fraude y estafa informática 147

Tabla 7. Resoluciones TASPIICJSJ sobre estafa informática del 2014 al 2019 161

Índice de gráficos

Gráfico 1. Antecedentes de la estafa informática..... 20

Gráfico 2. Resoluciones STCSJ sobre estafa informática 2014 al 2019..... 152

Lista de abreviaturas

CP	Código Penal
CPP	Código Procesal Penal
DRAE	Diccionario de la Real Academia Española
ed.	Edición
exp.	Expediente
INS	Instituto Nacional de Seguros
STCSJ	Sala Tercera de la Corte Suprema de Justicia
TASPIICJSJ	Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José

UNIVERSIDAD DE COSTA RICA

SEP Sistema de Estudios de Posgrado

Autorización para digitalización y comunicación pública de Trabajos Finales de Graduación del Sistema de Estudios de Posgrado en el Repositorio Institucional de la Universidad de Costa Rica.

Yo, Freddy Calderón Chaves, con cédula de identidad 1-1101-0724, en mi condición de autor del TFG titulado Construcción legislativa y aplicación jurisprudencial del delito de "Estafa" informática en Costa Rica del año 2014 al 2019. Énfasis en el uso indebido de datos.

Autorizo a la Universidad de Costa Rica para digitalizar y hacer divulgación pública de forma gratuita de dicho TFG a través del Repositorio Institucional u otro medio electrónico, para ser puesto a disposición del público según lo que establezca el Sistema de Estudios de Posgrado. **SI** [X] **NO** *[ ]

***En caso de la negativa favor indicar el tiempo de restricción: _____ año (s).**

Este Trabajo Final de Graduación será publicado en formato PDF, o en el formato que en el momento se establezca, de tal forma que el acceso al mismo sea libre, con el fin de permitir la consulta e impresión, pero no su modificación.

Manifiesto que mi Trabajo Final de Graduación fue debidamente subido al sistema digital Kerwá y su contenido corresponde al documento original que sirvió para la obtención de mi título, y que su información no infringe ni violenta ningún derecho a terceros. El TFG además cuenta con el visto bueno de mi Director (a) de Tesis o Tutor (a) y cumplió con lo establecido en la revisión del Formato por parte del Sistema de Estudios de Posgrado.

FREDDY CALDERON CHAVES (FIRMA)

Firmado digitalmente por FREDDY CALDERON CHAVES (FIRMA)
Fecha: 2022.05.02 19:21:06 -06'00'

FIRMA ESTUDIANTE

Nota: El presente documento constituye una declaración jurada, cuyos alcances aseguran a la Universidad, que su contenido sea tomado como cierto. Su importancia radica en que permite abreviar procedimientos administrativos, y al mismo tiempo genera una responsabilidad legal para que quien declare contrario a la verdad de lo que manifiesta, puede como consecuencia, enfrentar un proceso penal por delito de perjurio, tipificado en el artículo 318 de nuestro Código Penal. Lo anterior implica que el estudiante se vea forzado a realizar su mayor esfuerzo para que no sólo incluya información veraz en la Licencia de Publicación, sino que también realice diligentemente la gestión de subir el documento correcto en la plataforma digital Kerwá.

Introducción

El delito "estafa" informática tipificado en el artículo 217 bis del Código Penal costarricense (en adelante CP), nació a la vida jurídica mediante la ley N.º 9048 del 10 de julio de 2012, titulada: *"Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal"*, publicada en el Alcance N.º 172 de La Gaceta N.º 214 del 06 de noviembre de 2012.[1]

Dicha figura penal ha sido poco abordada en la dogmática penal costarricense, dentro de las pocas fuentes bibliográficas que podemos encontrar, relacionadas con delitos informáticos y por ende con la estafa informática, se cuenta con algunos artículos de revista; así como libros, entre ellos el publicado por el autor Roberto Lemaître Picado en el año 2011, titulado: *"Manual sobre delitos informáticos para la cibersociedad costarricense"*[2]; y propiamente sobre el tema en específico, se encuentra la obra *"La Estafa Informática"*, publicada en el año 2016 por el jurista nacional, doctor Francisco Castillo González. A pesar de lo anterior, existe un amplio espectro sobre dicha delincuencia que no ha sido visibilizado, como muestra de ello, el profesor Castillo menciona: *"…En Costa Rica carecemos de estudios sobre el perfil del estafador informático y de estadísticas fiables sobre la estafa informática..."*[3] Además, con respecto a una forma de comisión del delito señala: *"...Es esencial que el sistema automatizado de datos se encuentre en marcha (en funcionamiento). Esta característica de la estafa informática no ha sido puesta de manifiesto por la doctrina ni por la jurisprudencia*

[1] La Ley 9048 del 10 de julio de 2012 provocó la reforma del artículo 217 bis del Código Penal, el cual tipificaba antes de la "estafa informática" el delito denominado "fraude informático", que había sido construido mediante la Ley N° 8148 del 24 de octubre de 2001, publicado en La Gaceta el 21 de noviembre de 2001.

[2] Mientras desarrollaba el trabajo de investigación, se publicó la 2ª edición de dicho Manual, fuente bibliográfica que también será utilizada en la investigación.

[3] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p.52.

nacionales..."[4] En esa misma línea, se debe mencionar que no existe en la actualidad, ningún texto jurídico-penal crítico, que visibilice cuáles fueron los discursos generados dentro de la Asamblea Legislativa, desde finales del año 2009 y hasta el 2012, para la promulgación de la ley N.º 9048; así como la necesidad político-criminal que motivó propiamente la reforma del artículo 217 bis del CP, variando no sólo su contenido, sino también su nomenclatura de "fraude informático" a "estafa informática"; de igual manera, no existe ningún estudio con enfoque jurisprudencial de cómo se ha tratado en casos concretos el numeral 217 bis vigente. Precisamente, esos serán algunos de los aspectos a considerar en el desarrollo este trabajo, los cuales van de la mano con el estudio profundo de la estafa informática, abarcando aspectos medulares de dicha delincuencia, la cual no ha perdido relevancia después de siete años de promulgada la ley, más valorando que vivimos en la denominada sociedad de la información. Para dicha labor, se toman en cuenta fuentes bibliográficas a nivel internacional que han tratado el tema de la estafa informática, generando conocimiento importante que sin lugar a dudas ayudará al debate jurídico costarricense.

Ahora bien, debemos recordar que la informática es una expresión de la modernización, concepto último cuyo significado según el sociólogo, filósofo, psicólogo y politólogo alemán, Ulrich Beck consiste en *"innovaciones constantes"*[5], siendo además que: *"La modernidad, en su sistematicidad social e industrial, comporta un potencial de perjuicios que se originan sin pre-visión y en oposición abierta con la exigencia de racionalidad que ella misma reclama…"*[6] Dentro de esa coyuntura, la informática, como una disciplina en pleno apogeo que crea riesgos, se caracteriza por ser: Innovadora, evolutiva y tecnológica, siendo que día con día algunas personas se aprovechan de los sistemas tecnológicos para dañar el patrimonio de otras, tal y como lo refiere Ulrich Beck: *"Siempre hay «perdedores*

[4] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 85.

[5] BECK, Ulrich. *La sociedad del riesgo*. Traducción de M.ª Rosa Borrás y otros. Editorial Paidós, Barcelona, 1ª ed. 2019, p. 393.

[6] BECK, Ulrich. *La sociedad del riesgo*. Traducción de M.ª Rosa Borrás y otros. Editorial Paidós, Barcelona, 1ª ed. 2019, p. 395.

por el riesgo» y «vencedores por el riesgo»"[7], en ese sentido, la profesional en informática costarricense, máster Marta Eunice Calderón Campos, refiere: *"...Las noticias en los periódicos confirman que el ciberespacio, ese ámbito creado con tecnología de información y comunicación que es un "lugar de comunicación social transnacional, universal y en permanente evolución tecnológica" (Miró, 2011. p. 4), es muy propicio para cometer delitos de mucho impacto. Fraudes con tarjetas de crédito, datos confidenciales publicados sin el debido permiso, sustracción masiva de dinero de cuentas bancarias y páginas web alteradas son solo algunos ejemplos que muestran la existencia de vulnerabilidades -puntos débiles aprovechados por terceros para realizar ataques- en los sistemas de software y telecomunicaciones. Pese a que las organizaciones han establecido mecanismos de protección, estos parecen nunca ser suficientes..."*[8]

A pesar de esa realidad social en la que vivimos, la cual es propicia para la proliferación de tipos penales, en una expansión ilimitada del derecho penal en pro de la tan ansiada "seguridad ciudadana"[9] (en la que muchas veces el fin justifica

---

[7] BECK, Ulrich. *La sociedad del riesgo*. Traducción de M. ª Rosa Borrás y otros. Editorial Paidós, Barcelona, 1ª ed. 2019, p. 396.

[8] CALDERÓN CAMPOS, Marta Eunice. *Marco jurídico de la profesión informática en Costa Rica*. Editorial Universidad de Costa Rica (UCR), Costa Rica, 1ª ed. 2018, xiv, p. 39.

[9] Ver ANTILLÓN MONTEALEGRE, Walter. *El discurso de la seguridad ciudadana en las recientes reformas procesales*. En: Reflexiones jurídicas frente al populismo penal en Costa Rica. Editorial Investigaciones Jurídicas S.A., 1ª ed. San José, 2012, pp. 24 y 25: *"Se viene hablando de seguridad ciudadana en dos sentidos diferentes, incluso opuestos: a) como un derecho de todo ciudadano a que se le aseguren sus derechos fundamentales (derecho a los derechos: seguridad humana); es decir, el derecho a una prestación a cargo del Estado, que consiste en asegurar a todos el goce de sus derechos fundamentales, con especial atención en los derechos económicos, sociales y culturales, generalmente postergados (sobre ello: Alessandro Baratta: ´Seguridad´, en "Criminología y sistema penal"; BdeF, Montevideo, 2004; pág. 199 y sigtes.); y b) como término sinónimo de ´seguridad nacional´, es decir, como un intento de exhumar, con un nombre políticamente biensonante, aquella ominosa práctica de la época de la Guerra Fría; pero ahora posicionando en el centro de la mira: a) como ´enemigo actual y efectivo´ al que pueda ser considerado sospechoso de terrorismo en un sentido amplísimo, o de pertenecer a una organización criminal; y b) como ´enemigo potencial´ a cualesquiera otras personas, esto es, a la entera comunidad de ciudadanos que soportarán los controles, las escuchas, las injerencias y en fin, las medidas generales dispuestas a título de ´prevención´ (confr.: Jesús Fernández Entralgo – Guillermo Portilla Contreras – Javier Barcelona Llop: Seguridad ciudadana. Materiales de reflexión crítica sobre la ley Corcuera; Trotta, Madrid, 1993). En efecto, para justificar ese tipo de legislación, en la prensa diaria se invoca la seguridad de los ciudadanos honestos, que se ganan la vida con su trabajo (los buenos), como un valor a asegurar frente a la banda delincuencial que los atropella y los roba para comprar drogas (los malos); y se exige mano dura, aumento de las penas, cero*

los medios[10]), es esencial detenernos a pensar y cuestionarnos sobre la necesidad, utilidad e idoneidad de una figura penal como la estafa informática, es decir, ¿Deviene en útil para el entramado social en la solución de conflictos la redacción de ese tipo penal? En el hipotético caso de que la respuesta fuese afirmativa, cabe entonces cuestionarse si ¿Es proporcional la reacción o respuesta estatal a conductas como las que se describen en ese tipo penal 217 bis del CP?

La problemática que acarrea la delincuencia en estudio, tanto para las personas que legislan, para quienes operan el derecho y más importante aún, para quienes se les juzga, son extremos que pretendo abordar en esta investigación; mi intención es realizar un enfoque crítico de la realidad costarricense, desde todas esas perspectivas, haciendo énfasis en aquellos comportamientos humanos que implican fraudes mediante el uso indebido de datos, ya sea con tarjetas bancarias en cajeros automáticos, así como cualquier otra de sus manifestaciones.

Partiendo de lo anterior, se indagarán fuentes formales, tanto nacionales como extranjeras, en las que se exponen las distintas posiciones doctrinales que analizan el fenómeno de la estafa informática, dilucidando en un primer momento,

---

tolerancia. Y se reprocha a los jueces y fiscales su alcahuetería y sus paños tibios en el tratamiento a los antisociales; mientras que los defensores públicos son vistos como sus indudables cómplices (Conf.: IIDH: La seguridad ciudadana en Centroamérica. Aspectos teóricos y metodológicos, en AAVV.: "Derechos Humanos, proceso penal, seguridad ciudadana" s.f., pág. 184 y sigtes.). Y ¿qué ha dispuesto hacer el Estado para salvar a todos estos buenos padres de familia que piden ansiosamente seguridad? Como veremos más de cerca en el capítulo siguiente, lo que ya nos está ocurriendo en Costa Rica y en toda Centroamérica es que el Estado se ha colocado en posición que le permite atropellarnos legalmente, con la excusa de evitar que nos atropellen los delincuentes. La clave para entender esta aparente contradicción es que, en el fondo de las cosas, a las cúpulas del poder no les interesa tanto el delincuente como el inconforme contestatario; no le interesa tanto el delito (el cadenazo, las maras) como la protesta, la disensión y la oposición (la huelga de Sintrajup) contra las grandes operaciones macroestatales proyectadas por el capital transnacional."

[10] Ver CHIRINO SÁNCHEZ, Alfredo. *Las Tecnologías de la información y el Proceso Penal. Análisis de una crisis anunciada*. En: Revista de la Asociación de Ciencias Penales de Costa Rica., año 9, n° 14, San José, 1997, p. 43: *"Se habla de que la guerra contra la criminalidad sólo la podrá ganar el Estado si es eficiente, y para ello resulta necesario confiarle más herramientas y más posibilidades de acción, mayores facultades para escoger lo que persigue y más y mejores recursos para realizar esta tarea. En esta carrera por la "eficiencia" no se duda en potenciar la necesidad de reducir garantías clásicas en favor del imputado, cuando las mismas resultan sospechosas de reducir la "eficiencia" de la reacción estatal, o cuando un respeto de éstas acarree una disminución de las posibilidades de éxito frente a la criminalidad."*

si es correcto y adecuado, a la luz del principio de legalidad, denominar lo descrito en el numeral 217 bis del CP, como una especie de “estafa”, o si por lo contrario, debió denominarse a esa descripción objetiva de la conducta de manera distinta, develando entonces si esa titulación resulta un dato meramente nominal e inofensivo, o por el contrario, si genera consecuencias jurídicas significativas.

Es allí donde toma especial importancia sumergirnos en las discusiones legislativas, para indagar cuáles elementos fueron ponderados para redactar la norma; si las personas legisladoras tuvieron claros los argumentos jurídicos de fondo para promulgar la ley; cuáles fueron sus motivaciones sociológicas, políticas y de persecución criminal, no sólo al describir una conducta humana en el numeral 217 bis del CP, sino al tratarla como una estafa. Es imprescindible conocer si justificaron por qué el delito de “fraude informático” debía ser reformado. Asimismo, ¿por qué a pesar de la existencia de la estafa general, era necesario construir un nuevo tipo penal, denominado “estafa informática”?

En términos generales, sería relevante visibilizar o conocer, si quienes redactaron el tipo penal informático, manejaron las diferencias técnico-jurídicas entre la estafa general (216 del CP) y lo descrito en el numeral 217 bis del mismo cuerpo normativo, ello con la posible intención de no incurrir en una duplicación de tipos penales, ese extremo además de básico, pareciera medular en el análisis de idoneidad, pertinencia y necesidad de la norma penal, como lo hace ver el autor González Rus con respecto a los delitos informáticos en general y la estafa informática en particular: *“Las formas de comisión posibles son tantas y tan diversas y las figuras delictivas que pueden verse implicadas tan distintas (hurto, robo, estafa, daños, falsificaciones, descubrimiento de secretos de empresa, utilización ilegítima de terminales de telecomunicación, defraudaciones de la propiedad intelectual, etc.) que los intentos de clasificación resultan particularmente complicados. Un mismo procedimiento comisivo puede dar lugar, según los casos, a diversos tipos de fraude o manipulación, pudiendo ser analizado desde la perspectiva de varios y distintos delitos, según la ocasión; del mismo modo que, en otras, el uso de la informática no supone más que un modus*

operandi nuevo que no plantea particularidad alguna respecto de las formas tradicionales de comisión"[11].

En virtud de ello, es requisito obligatorio de esta tesis, realizar un análisis comparativo, entre la estafa general y la estafa informática, para determinar si la segunda prevé escenarios fácticos diversos a la primera. Es decir, la reflexión propiamente dicha será, si realmente la estafa informática es un tipo penal vigente, pero sin eficacia, o si contempla supuestos fácticos nuevos que, ameritaban crear un tipo penal, precisamente para ello se analizaran resoluciones de la Sala Tercera de la Corte Suprema de Justicia (en adelante STCSJ) y del Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José (en adelante TASPIICJSJ), del año 2014 al 2019.

Indispensable es el tema del bien jurídico tutelado, el cual será explorado en el presente trabajo, con la finalidad de descubrir, el por qué y para qué se construyó el delito de estafa informática, analizando por ende si estamos ante un tipo penal que tutela un único bien jurídico o si por el contrario es pluriofensivo, así como las posibles repercusiones que tendría al momento de analizar la antijuridicidad material y el principio de lesividad, ello bajo la sombra de la Teoría General del Delito.

Un tema vinculado con la estafa informática es la circulación de tarjetas bancarias[12] en nuestra sociedad. La fotografía de la realidad costarricense

---

[11] GONZÁLEZ RUS, Juan José. *Protección Penal de Sistemas, Elementos, Datos, Documentos y Programas Informáticos*. En: Revista Electrónica de Ciencia Penal y Criminología, RECPC 01-14 (1999), ISSN 1695-0194. Madrid, 1999. En: http://criminet.ugr.es/recpc/recpc_01-14.html.

[12] Ver sitio web de la Presidencia de la República de Costa Rica: https://presidencia.go.cr/comunicados/2019/03/en-nueve-anos-tarjetas-de-credito-aumentaron-un-125, consulta realizada el 13-11-2019, se indica: *"...El último estudio trimestral de tarjetas de crédito y débito, con corte al 31 de octubre del 2018, realizado por el Ministerio de Economía, Industria y Comercio (MEIC), por medio de la Dirección de Investigaciones Económicas y de Mercados, determinó que en nueve años, la cantidad de tarjetas crédito en el país aumentó un 125%, lo que representa un total de 2.984.769 plásticos en circulación de los cuales 1.976.522 son titulares y 1.008.247 son plásticos adicionales, es decir ligados a un tarjetahabiente titular. En octubre del 2011 se presentó la menor variación interanual (4,3% con respecto a octubre 2010), posteriormente, se observa una tendencia creciente en la cantidad de tarjetas colocadas, siendo octubre del 2018 el período con el mayor crecimiento interanual (del 13,5%). Por su parte, el crecimiento anual promedio de la cantidad de tarjetas en circulación ha sido de un 9,4% durante el*

respecto al número de éstas en circulación al 31 de enero de 2020 fue el siguiente: 2.944.009 de crédito y 5.749.072 de débito[13]. Esas cifras abren el margen de ser víctima de que un plástico pueda ser usado sin autorización del titular, provocando el surgimiento de formas varias de defraudación mediante dichos instrumentos[14], ese sin lugar a dudas, es un tema que merece ser indagado, no sólo por la trascendencia actual, en virtud del amplio espectro de supuestos en los que se puede hacer uso de una tarjeta para defraudar a una persona, sino además, en la misma tipificación de conductas, ya sea que se les considere: Hurto, robo, uso de documento falso, falsificación de valores equiparados a la moneda, estafa básica, o estafa informática.

Otra realidad nacional que acrecienta las posibilidades de sufrir una defraudación mediante Internet, es precisamente la cantidad de población usuaria de dicha red, ya sea a través de dispositivos celulares o de Internet fijo, que al cerrar el año 2018, alcanzó las siguientes suscripciones: 4.858.940 y 834.784, respectivamente, datos que hablan por sí solos, en tanto evidencian que la mayor cantidad de personas están constantemente navegando en la web[15], vale mencionar en ese sentido que Costa Rica en el año 2016, se ubicó en los

---

período en análisis. Cantidad de tarjetas de crédito en circulación y su respectiva variación por año, con corte al 31 de octubre 2018...", estudio completo en sitio web del Ministerio de Economía, Industria y Comercio: http://reventazon.meic.go.cr/informacion/estudios/2018/tarjetas/octubre/pcp.pdf. En octubre de 2019, el número de tarjetas de crédito y débito en circulación fue de 2.947.141 y 5.855.219, respectivamente, ver: http://reventazon.meic.go.cr/informacion/estudios/2019/tarjetas/octubre/pcp.pdf.

[13] Ver sitio web: http://reventazon.meic.go.cr/informacion/estudios/2020/tarjetas/enero/ppc.pdf.

[14] Ver ejemplos de actuaciones delictivas en cajeros automáticos en: MONGE GÓMEZ, Marco. *Cajeros automáticos ¿amigos o enemigos?* En: Revista investigación y ciencia. Organismo de Investigación Judicial, 2ª ed. ISSN 2215-2547. Versión electrónica en: https://sitiooij.poder-judicial.go.cr/index.php/comunicacion/publicaciones/revistas-investigacion-y-ciencia-edicion/item/6691-revista-investigacion-y-ciencia-edicion-n-2, 2012, pp. 5 y 6.

[15] SUPERINTENDENCIA DE TELECOMUNICACIONES. *Estadísticas del sector de telecomunicaciones,* 1ª ed. digital, San José, 2019. Versión electrónica en: https://sutel.go.cr/sites/default/files/informe_estadisticas_del_sector_de_las_telecomunicaciones_2018_vf.pdf, pp. 90 y 92.

primeros tres puestos de países con mayor cantidad de hogares con acceso a Internet[16].

En resumen, la investigación pretende estudiar y analizar la figura penal de la "estafa" informática, con la intención de fomentar el conocimiento mediante el debate jurídico nacional. Además, acercarnos a la realidad costarricense, pretendiendo ser una herramienta de utilidad para quienes muestran interés en la denominada delincuencia informática y específicamente en la "estafa" informática.

Como una precisión conceptual, es importante mencionar que, cuando sea usado el concepto "estafa informática", me estaré refiriendo a la redacción actual del 217 bis del CP; y cuando haga alusión al "fraude informático", estaré acotando al antiguo 217 bis del CP. Tal y como se expondrá, ambas figuras penales tienen redacciones distintas, y aunque la estafa informática pueda ser catalogada como un tipo de fraude informático, no todo fraude informático es una estafa informática, similar situación acontece con la estafa general y el concepto de defraudación[17]. El hecho de usar ambos conceptos de manera indiscriminada, confundiendo uno con el otro, provoca imprecisiones importantes, tal y como se verá en el transcurso de la investigación.

En virtud de todo lo anterior, la presente tesis consiste en una investigación desde un enfoque cualitativo[18], cuyas hipótesis de trabajo son las siguientes:

---

[16] Ver: 1) SUPERINTENDENCIA DE TELECOMUNICACIONES. *Costa Rica con mayor cantidad de hogares con acceso a internet en la región*. Versión electrónica en: https://sutel.go.cr/noticias/comunicados-de-prensa/costa-rica-con-mayor-cantidad-de-hogares-con-acceso-internet-en-la., 2016. 2) COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE. *Estado de la banda ancha en América Latina y el Caribe 2016*. Naciones Unidas, CEPAL, cooperación alemana, 2016. Versión electrónica en: https://repositorio.cepal.org/bitstream/handle/11362/40528/6/S1601049_es.pdf, p. 10

[17] Ver DONNA, Edgardo Alberto y DE LA FUENTE, Javier Esteban. *Aspectos generales del tipo penal de estafa*. En: Revista Latinoamericana de Derecho, año I, N° 1, 2004, p. 48: *"Es importante aclarar que por defraudación se debe entender "toda lesión patrimonial producida con fraude", de modo que se trata del "género", cuyas especies son la estafa […] modalidades que resultan claramente diferentes."*

[18] Ver ULATE SOTO, Ileana y VARGAS MORÚA, Elizarda. *Metodología para elaborar una tesis*. EUNED. 1ª ed. San José, 2016, p. 5. *"La investigación cualitativa, la cual se ubica a finales del siglo XIX e inicios del siglo XX, es una corriente influida en parte por el contructivismo, este*

Hipótesis I: La redacción utilizada por las personas legisladoras al denominar estafa informática a la acción de introducir datos en un sistema informático, no concuerda con lo que ha dicho la doctrina que debe entenderse por estafa.

Hipótesis II: El tipo penal de estafa informática confunde en su formulación varios conceptos, en primer lugar, la tesis del error de la máquina, deficiencias al utilizar distintos verbos típicos, así como falencias por ubicar como objeto de la acción delictiva el procesamiento de datos.

Hipótesis III: El tipo penal de la estafa informática, conlleva serios problemas de aplicación, pues su construcción, deja a la libre interpretación judicial, el problema de la manipulación de datos para obstaculizar un proceso válido de datos, además, deja como un problema de un concurso aparente de tipos penales, otras formas de comisión de delitos informáticos.

Hipótesis IV: Ni las resoluciones de la Sala Tercera ni del TASPIICJSJ, referentes al delito de estafa informática, se ajustan a la regulación normativa ni doctrinaria del delito en mención, dejando de lado principios constitucionales.

Por su parte, me propuse los siguientes objetivos:

Objetivo general: Indagar sobre las diferencias y similitudes entre el delito de estafa y de estafa informática, con la finalidad de determinar, si la estafa informática costarricense contempla supuestos fácticos diferentes al tipo penal base de estafa.

Objetivos específicos:

1. Precisar el tratamiento teórico dogmático dado a la estafa informática en nuestro país, así como en Alemania, Argentina y España, enfocado en el uso indebido de datos y en relación con el bien jurídico tutelado.

---

propone que no hay una realidad objetiva, sino que esta es edificada socialmente a través de construcciones medibles. El conocimiento es construido por las personas que participan en la investigación, de tal forma que los individuos y el investigador se involucran en un proceso interactivo (Hernández et al., 2010).”

2. Establecer si la nomenclatura dada en Costa Rica al delito de estafa informática es la más precisa desde el punto de vista analítico, y si se corresponde con la doctrina estudiada, en cuanto a lo que se debe entender por estafa.

3. Analizar el tipo penal de estafa informática previsto en el artículo 217 bis del CP, para determinar si mejora, amplía o profundiza de alguna manera el tipo penal base de estafa del artículo 216 del mismo cuerpo normativo. Comparar la dosimetría penal entre ambas delincuencias y las implicaciones procesales.

4. Establecer desde un punto de vista normativo, si el error en la máquina y la manipulación de datos en un sistema informático configura una acción estafadora.

5. Determinar empíricamente, cuáles fueron los argumentos que tomó en cuenta la persona legisladora para la construcción normativa del tipo penal de estafa informática.

6. Estudiar desde un enfoque empírico, el tratamiento jurisprudencial dado a la estafa informática por la STCSJ y el TASPIICJSJ, durante los años 2014 al 2019, enfocando la atención en los casos en que se hizo uso indebido de datos. Visibilizar el perfil de los sujetos activos de la conducta que logra captar nuestro sistema punitivo.

Metodología:

La presente investigación tiene como objeto de estudio el tipo penal de estafa informática, el cual será abordado desde tres niveles de análisis: el primero de ellos teórico dogmático; el segundo normativo; y, por último, de carácter empírico.

El método de análisis iniciará con la dimensión teórico-dogmática, se ocupará el estudio de fuentes formales que traten el tema tanto a nivel nacional como internacional de la estafa informática. Asimismo, será necesario realizar

estudio de derecho comparado, para conocer el tratamiento que en otras latitudes se le ha dado al tema de la estafa informática, tomando en cuenta a los países de Alemania, Argentina y España.

A nivel normativo y mediante una investigación exploratoria, tanto descriptiva como explicativa, se analizarán las actas legislativas, mediante las cuales se aprobó la ley N° 9048 del 10 de julio de 2012, cuerpo legal que contempló el delito de estafa informática.

Asimismo, se recolectarán y de manera explicativa se analizarán, desde un diseño de casos múltiples[19], aquellas resoluciones de mayor trascendencia emitidas durante los años 2014 al 2019 por STCSJ y el TASPIICJSJ, relacionadas con la estafa informática, realizando una investigación exploratoria del tema, siendo descriptiva y explicativa a la vez.

De esa manera, se incorpora a la investigación un orden sistemático y con triangulación[20], que permite la comprensión y el análisis de la figura en estudio, en procura de alcanzar adecuadamente el conocimiento desde adentro del objeto de estudio, y resolver los problemas que el tipo penal de estafa informática le genera tanto a las personas operadoras del derecho como a quienes son usuarias del sistema penal costarricense.

---

[19] Ver BARRANTES ECHAVARRÍA, Rodrigo*. Investigación: un camino al conocimiento, un enfoque cualitativo, cuantitativo y mixto*. EUNED. 2ª ed. San José, 2016, p. 229: *"No obstante, hay diseño de casos múltiples, en donde se analizan varios casos a la vez, para estudiar una realidad que se desea explorar, describir, evaluar o modificar. Estos estudios son más convincentes y más "robustos", al basarse en la replicación (capacidad de contestar y de contrastar las respuestas obtenidas, de forma parcial, con cada caso que se analiza).*

[20] Ver BARRANTES ECHAVARRÍA, Rodrigo*. Investigación: un camino al conocimiento, un enfoque cualitativo, cuantitativo y mixto*. EUNED. 2ª ed. San José, 2016, p. 135: *"La triangulación es la mezcla de dos o más teorías, fuentes de datos, técnicas de investigación, en el estudio de un fenómeno singular, o sea, es el uso de diferentes formas de estudiar un mismo objeto."*

Capítulo I. Tratamiento de la estafa informática a nivel doctrinal

Es sabido que la informática es un fenómeno cambiante, se encuentra en constante evolución[21], no solamente abarca acciones concernientes a la información, sino que está íntimamente ligada con el desarrollo computacional, sus nuevas tendencias y tecnologías; ello implica que el derecho penal al considerarla dentro de su margen de acción, requiera adaptarse a esas nuevas corrientes, nótese que *"...Las computadoras y las telecomunicaciones han invadido todas las actividades humanas; han sido utilizadas para ofrecer grandes beneficios a la humanidad y crear oportunidades en muchos ámbitos [...] La normativa jurídica se actualiza a un paso mucho más lento que el de la tecnología de información. Esto se agrava porque los seres humanos son muy creativos y pronto encuentran formas de uso, no todas lícitas, que no fueron pensadas por los creadores de la tecnología..."*[22] Podemos afirmar entonces que, con el advenimiento de la informática como una nueva forma de energía y de poder[23], el

[21] Ver S. MARTÍNEZ, Matilde. *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*. Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 33: *"...Las Tecnologías de la Información y Comunicación (TIC), seguidas de una vertiginosa evolución, han generado una nueva forma de poder, "el poder informático". Este nuevo poder no ha sido indiferente al derecho, que debe adoptar, por un lado, la postura de legitimarlo en virtud de los magníficos beneficios que proporciona a los individuos; por otro lado, debe adoptar una postura contenedora, debido a los peligros que puede ocasionar a las personas. Se van creando nuevas herramientas jurídicas tendientes a la protección frente a los abusos de este nuevo poder..."*

[22] CALDERÓN CAMPOS, Marta Eunice. *Marco jurídico de la profesión informática en Costa Rica*. Editorial Universidad de Costa Rica (UCR), Costa Rica, 1ª ed. 2018, pp. ix-x.

[23] Ver FROSINI, Vittorio. *Cibernética, Derecho, Internet y Sociedad*. Ediciones Olejnik, Santiago-Chile, 1ª ed. 2019, pp. 113-114: *"La informática señala, por esta razón, una tercera fase en la historia de la comunicación hablada del hombre. La primera fase ha sido la de la palabra oral, es decir, la del lenguaje no gestual, sino fonéticamente articulado según ciertas reglas socialmente aceptadas. La segunda fase ha sido la de la palabra escrita, es decir, del lenguaje separado de su expresión natural de comunicación de hombre a hombre, de audible transformado en visible, realizado, es decir, hecho una cosa, un objeto que puede sobrevivir a los hombres qué lo hablaron (como el caso de las así llamadas lenguas muertas) y que puede ser transmitido en el tiempo y el espacio sin necesidad de ser transportado por el hombre (como es el caso del manuscrito contenido en una botella). La tercera fase, que ha sido preparada por el desarrollo del lenguaje matemático, es la del lenguaje electrónico como conjunto de señales simbólicas de palabras, que no es un lenguaje hablado ni escrito, sino que se trata de un metalenguaje comunicado por medio de las máquinas; se podría decir: de un lenguaje totalmente artificial. La informática representa de tal modo la conquista de una nueva forma de energía, no física sino intelectual, de la Humanidad, que nos acrecienta y multiplica de manera inesperada la posibilidad del desarrollo científico y social*

derecho se vio en la necesidad de adaptar su teoría: 1) A la protección de datos y de información digital como bienes jurídicos; 2) Al uso de dispositivos automatizados para el mejoramiento de procesos administrativos.[24] Vale mencionar que nos encontramos ante una paradoja[25], por un lado el desarrollo y avance de la informática facilita la vida de las personas, pero por el otro, se convierte en un riesgo para diferentes intereses del ser humano, siendo el mismo *homo sapiens*, quien debe crear prácticas de mitigación de esos riesgos. Es un hecho que la sociedad del siglo XXI se desenvuelve en el modelo capitalista, con todo lo que ello implica, un ser humano construido socialmente para producir[26] y consumir[27], convirtiéndose la capacidad económica en un valor no sólo material, sino además social y simbólico, que cambia las relaciones de poder[28], además, termina siendo el núcleo sobre el cual giran las vidas humanas[29], es en ese

---

[…] Como toda forma de energía, física o psicológica, también la energía intelectual de la informática constituye una forma de poder […] Este nuevo poder puede ser concentrado o difundido en una sociedad, confiado a la iniciativa privada o reservado al monopolio estatal, concebido como un nuevo tejido cohesionador de la sociedad civil o como un instrumento de sumisión universal, y sobre esta alternativa de empleo de la nueva técnica de conocimiento y de poder se juega el destino social del hombre de hoy."

[24] SAIN, Gustavo. *La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas más allá de la solución penal*. Cibercrimen y delitos informáticos. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 12.

[25] BECK, Ulrich. *La sociedad del riesgo*. Traducción de M. ª Rosa Borrás y otros. Editorial Paidós, Barcelona, 1ª ed. 2019, p. 332: *"En aquellos aspectos en que los riesgos preocupan a los hombres ya no se da un peligro cuyo origen quepa atribuirlo a lo externo, a lo ajeno, a lo extrahumano, sino a la capacidad adquirida históricamente por los hombres de autotransformar, de autoconfigurar y de autodestruir las condiciones de reproducción de toda la vida sobre la tierra…"*

[26] BECK, Ulrich. *La sociedad del riesgo*. Traducción de M. ª Rosa Borrás y otros. Editorial Paidós, Barcelona, 1ª ed. 2019, p. 383: *"…de modo que el control sobre el proceso de producción comienza a depender esencialmente de los finos hilos de la accesibilidad a las redes de información…"*

[27] BECK, Ulrich. *La sociedad del riesgo*. Editorial Paidós, Barcelona, 1ª ed. 2019, p. 386. *"…La ola de automatización microelectrónica produce formas mezcladas de trabajo remunerado y sin remunerar, formas en las cuales la parte de trabajo mediado por el mercado disminuye y en cambio aumenta la parte de autotrabajo orientado al consumo. La ola de automatización en el sector de servicios cabe, pues, concebirla como un desplazamiento de trabajo de la producción al consumo, de los especialistas a la generalidad, de la remuneración a la autoparticipación…"*

[28] BECK, Ulrich. *La sociedad del riesgo*. Editorial Paidós, Barcelona, 1ª ed. 2019, p. 144.

[29] BECK, Ulrich. *La sociedad del riesgo*. Editorial Paidós, Barcelona, 1ª ed. 2019, p.p 116-117: *"Para la supervivencia en la vieja sociedad industrial es central la capacidad de los seres humanos*

contexto, en el que las herramientas tecnológicas facilitan distintas transacciones bancarias pero todas vinculadas con la información: Transferencias de dinero, pagos de servicios, adquisición de bienes de manera electrónica, uso de tarjetas bancarias y otros, lo cual implica necesariamente una atmósfera riesgosa en la que de alguna manera se pierde el control sobre las acciones realizadas (por ejemplo: no es lo mismo poseer el dinero de forma material que virtual), convirtiéndose en caldo de cultivo para que algunas personas, de forma hábil e ilícita se aprovechen de esa información.

Si considerásemos el desarrollo tecnológico propio de la misma evolución del *Homo sapiens* y su "hegemonía"[30] sobre el resto de especies, se determina como consecuencia que, la humanidad se encuentre en un profundo proceso de transformación, en el cual, la "persona tecnológica", se convierte en una realidad tangible en la sociedad contemporánea, creándose una simbiosis vital con las máquinas que asisten en gran cantidad de labores cotidianas.[31] Y es que precisamente *"en la sociedad del siglo XXI se ha producido el tránsito de la era industrial a la de la información, nuestra economía se ha convertido en una*

---

de combatir la miseria material, de evitar el descenso social […] En la sociedad del riesgo se vuelven necesarias para la vida, adicionalmente, otras capacidades. Un peso esencial lo adquiere aquí la capacidad de anticipar peligros, de soportarlos, de enfrentarse a ellos biográfica y políticamente […] De este modo, en la sociedad del riesgo el trato con el miedo y con la inseguridad se convierten biográfica y políticamente en una cualificación civilizatoria clave, y la formación de las capacidades relativas a ello se convierte en una tarea esencial de las instituciones pedagógicas..." En la actualidad se mantiene esa misma realidad, estar en una miseria material implica necesariamente el cierre de muchas opciones de vida inclusive de supervivencia, por otro lado, el hecho de tener suficiente capacidad adquisitiva desde un punto de vista simbólico, provoca estatus social e incluso codicia, es decir, en pleno Siglo XXI, las motivaciones que llevan al ser humano a buscar tener capital son variadas, siendo sin lugar a dudas, unas más importantes que otras, indistintamente de ello, el patrimonio termina siendo un bien que al verse afectado provoca una reacción estatal, tal y como se hace por ejemplo con la estafa informática.

[30] HARARI, Yuval Noah. *Sapiens. De animales a dioses*. Traducción de Joandomènec. Editorial Penguin Random House, 5ta ed. 2017, pp. 90 y 98: *"…En la época de la revolución cognitiva vivían en el planeta unos 200 géneros de animales terrestres grandes que pesaban más de 50 kilogramos. En la época de la revolución agrícola solo quedaban alrededor de 100. Homo sapiens llevó a la extinción a cerca de la mitad de las grandes bestias del planeta mucho antes de que los humanos inventaran la rueda, la escritura o las herramientas de hierro […] Los culpables fueron un puñado de especies de plantas, entre las que se cuentan el trigo, el arroz y las patatas. Fueron estas plantas las que domesticaron a Homo sapiens, y no al revés…"*

[31] BÉHAR QUIÑONES, Gastón y YÁÑEZ FIGUEROA, Agustín. *Introducción a los contratos tecnológicos*. Editorial Tecnológica de Costa Rica, 1ª ed. Cartago, 2017, p. 9.

economía de la información. La era industrial se basó en la producción, mientras que la era de la información se fundamenta en la comunicación y la información electrónica, ambas a gran escala."[32] En ese sentido, es esencial entender que la información *"Es una agregación de datos que tiene un significado específico más allá de cada uno de estos". Tendrá un sentido particular según cómo y quién la procese. Por ejemplo, 1, 9, 8 y 7 son datos; su agregación 1987 es información"*.[33]

El concepto de Cibernética toma especial relevancia cuando de información se trata: *"En 1948, el matemático estadounidense Norbert Wienner, en su libro Cibernética o el control y comunicación en animales y máquinas, habla de una nueva disciplina para la organización de la sociedad sobre la base de una nueva materia prima: la información. Esta, junto a las máquinas y las redes, debía actuar en contra de la entropía, la tendencia natural a precipitar la degradación biológica y el desorden social."*[34] De esa manera, el matemático estableció un vínculo entre cibernética y derecho. La cibernética se puede definir entonces como *"ciencia del control y de la comunicación en los animales y en las máquinas"*[35]*.* Dicho autor, Norbert Wiener, en su siguiente obra denominada *"The Human Use of the Human Beings"* (1950), citada por Vittorio Frosini, puso en evidencia que *"los problemas jurídicos son, por naturaleza propia, problemas de comunicación y de cibernética;*

[32] S. MARTÍNEZ, Matilde. *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 33.

[33] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 50.

[34] SAIN, Gustavo. *La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas más allá de la solución penal*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 12.

[35] FROSINI, Vittorio. *Cibernética, Derecho, Internet y Sociedad*. Ediciones Olejnik, Santiago-Chile, 1ª ed. 2019, pp. 21 y 22.

esto es, son problemas relativos al control regular y repetible de ciertas situaciones críticas".[36]

En ese sentido, lo dicho por el autor Ulrich Beck en su libro *"La sociedad del riesgo"*, no pierde vigencia, ese margen de riesgo expuesto, no sólo persiste, sino que se ha acrecentado en otras situaciones cotidianas, pudiéndose considerar entre ellas la informática. Para una mejor claridad de lo expuesto, el autor citado señaló: *"...No sucede lo mismo con la sociedad del riesgo. Su contraproyecto normativo, que está a su base y la estimula, es la seguridad. En lugar del sistema axiológico de la sociedad «desigual» aparece, pues, el sistema axiológico de la sociedad insegura. Mientras que la utopía de la igualdad contiene una multitud de fines positivos de los cambios sociales, la utopía de la seguridad resta peculiarmente negativa y defensiva: en el fondo, aquí ya no se trata de alcanzar algo «bueno», sino ya sólo de evitar lo peor. El sueño de la sociedad de clases significa que todos quieren y deben participar en el pastel. El objetivo de la sociedad del riesgo es que todos han de ser protegidos del veneno..."*[37] Continúa indicando: *"...tal posibilidad ilustra de inmediato el pensamiento, que aquí es central, de que la sociedad industrial (además de la capitalista también la «socialista») produce sistemáticamente su propia amenaza y su propia debilidad estructural a través de la potenciación y la explotación económica de los riesgos. La situación histórico-social y su dinámica es perfectamente comparable con la situación del final del feudalismo en el umbral hacia una sociedad industrial. La nobleza feudal vivía de la economía burguesa (de la concesión de dependencia feudal de los derechos mercantiles y de usufructo, así como de los impuestos por la actividad industrial) y la promocionaba por su propio interés, creando, necesaria e involuntariamente, a su cada vez más poderoso sucesor. De la misma manera la sociedad industrial se «nutre» desde los propios riesgos que produce, creando de*

---

[36] FROSINI, Vittorio. *Cibernética, Derecho, Internet y Sociedad*. Ediciones Olejnik, Santiago-Chile, 1ª ed. 2019, pp. 21 y 22.

[37] BECK, Ulrich. *La sociedad del riesgo. Hacia una nueva modernidad*. Traducción de M. ª Rosa Borrás y otros. Editorial Paidós Ibérica, S.A., Barcelona, 1998. p. 55.

este modo situaciones de peligro social y peligros políticos potenciales que cuestionan las bases de la modernización conocidas hasta ahora..."[38]

Ahora bien, para prevenir ser víctima de un delito informático tal y como lo es la estafa informática, sale a relucir el concepto de "seguridad informática"[39], la cual si bien no es infalible, sí se convierte en una herramienta de mitigación a ese riesgo provocado por el mismo ser humano. Considera en ese sentido el autor Marcelo Temperini que, la totalidad de hechos no deseados donde se comprometa de alguna manera la seguridad de la información termina siendo un incidente de seguridad; lo cual le lleva a concluir que todos los delitos informáticos, en el fondo son **incidentes de seguridad de la información**[40], tema que se abordará en esta investigación cuando se analice el tópico del bien jurídico de la estafa informática del 217 bis del CP. Por el momento, es necesario mencionar que paradójicamente y sobre la necesidad de la seguridad informática, existen muchas plataformas informáticas de diferentes entidades o instituciones que almacenan datos o información sensible de personas, lo cual puede deparar (dependiendo del uso que se les dé) en consecuencias negativas para éstas, y es que precisamente esas fuentes de información tienen personas que las administran, entonces, cabe plantearse la interrogante: ¿Quién controla al que controla? En la actualidad sabemos que los datos se almacenan en un mundo paralelo invisible, como lo es

---

[38] BECK, Ulrich. *La sociedad del riesgo. Hacia una nueva modernidad*. Traducción de M. ª Rosa Borrás y otros. Editorial Paidós Ibérica, S.A., Barcelona, 1998. p. 64.

[39] Ver CALDERÓN CAMPOS, Marta Eunice. *Marco jurídico de la profesión informática en Costa Rica*. Editorial Universidad de Costa Rica (UCR), Costa Rica, 1ª ed. 2018, p. 39: *"...En este capítulo se utilizan los términos seguridad informática y ciberseguridad indistintamente. El objetivo de la primera es "reducir la probabilidad de materialización de las amenazas; limitando los daños o averías resultantes; y logrando que se reanuden las operaciones normales tras un incidente de seguridad, en un plazo de tiempo razonable y a un coste aceptable" (Unión Internacional de Telecomunicaciones, 2007, p. v). Por su parte, la ciberseguridad tiene como objetivo "contribuir a la preservación de las fuerzas y medios organizativos, humanos, financieros, tecnológicos e informativos, adquiridos por las instituciones, para realizar sus objetivos" (Unión Internacional de Telecomunicaciones, 2007, p. v). Ambos conceptos contemplan los procesos, los métodos y las técnicas para la protección del software, el hardware, las redes de telecomunicaciones, la infraestructura tecnológica y los servicios brindados mediantes (sic) todos los anteriores..."*

[40] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 50.

la denominada “nube” o la misma Internet, lo cual de alguna u otra manera representa un riesgo para nuestros intereses personales, económicos y sociales: *“…Precisamente con el crecimiento de los peligros surgen en la sociedad del riesgo desafíos completamente nuevos a la democracia. La sociedad del riesgo contiene una tendencia a un totalitarismo «legítimo» en la defensa contra los peligros, el cual con el pretexto de impedir lo peor crea todavía. Los «efectos secundarios» políticos de los «efectos secundarios» civilizatorios amenazan al sistema político-democrático en su sustancia, el cual cae de este modo en el dilema de o fracasar a la vista de los peligros producidos sistemáticamente o derogar principios democráticos básicos mediante «contrafuertes» autoritarios, propios de un Estado de orden. Reventar este dilema es una de las tareas esenciales del pensamiento y de la actuación democráticos en el futuro presente de la sociedad del riesgo…”*[41]

En la actualidad y desde la década de los años 80, con la irrupción de Internet, se acuña el concepto de sociedad de la información, que impactó la forma de comunicación entre seres humanos. Asimismo, el comercio, el tratamiento y almacenamiento de datos, los correos electrónicos, la bancarización digital del tráfico económico, los contratos electrónicos, son situaciones que develan la dependencia del ser humano con las computadoras.[42] A ello se le agrega *“...un nuevo nivel en la forma de comisión de estos delitos que viene posibilitada de la mano de las características propias de las nuevas tecnologías que anteriormente citábamos (inmediatez a distancia, masividad y anonimato). Por ejemplo, un estafador clásico debía tomar sus recaudos en el tipo de engaño, acercarse a la víctima, teniendo las habilidades sociales necesarias, hacer incurrir en el error a la víctima y, así, lograr llevar adelante una estafa. Todos estos pasos resultan casi automatizados en las estafas electrónicas, donde las posibilidades de*

[41] BECK, Ulrich. *La sociedad del riesgo. Hacia una nueva modernidad*. Editorial Paidós Ibérica, S.A., Barcelona, 1998, pp. 121-122.

[42] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. XXV.

éxito del delincuente aumentan radicalmente. A través de las herramientas tecnológicas, desde cualquier lugar con conexión a Internet (realización a distancia), el delincuente podrá atacar múltiples víctimas a la vez (masividad), enviando cientos de correos electrónicos a la vez, de forma instantánea (no se necesita esperar), y, de acuerdo con el nivel de conocimiento del delincuente, hasta podrá utilizar determinados mecanismos que obstaculicen su rastreo o identificación (anonimato) […] las tecnologías son potenciadoras de determinados tipos de delitos, que no son nuevos, pero que, al combinarse con las características de las nuevas tecnologías de la información, terminan llevando el delito a un nuevo nivel de desarrollo..."[43]

Siempre dentro del recuento histórico, el jurista Ulrich Sieber, citado por Gustavo Sain, refirió: *"En cuanto a los fraudes de tipo financiero, a fines de la década de 1970 y a principios de la década de 1980, hubo casos de alteración de archivos de las bases de datos empresariales y los balances bancarios con el fin de manipular las facturas de pagos de salarios. Casos típicos se realizaban mediante la instalación de dispositivos lectores en las puertas de entrada a los cajeros automáticos y mediante teclados falsos para la copia de los datos de las tarjetas de débito a través de la vulneración de las bandas magnéticas. Esto motivó, por parte de las empresas emisoras, la adopción de chips, en los plásticos, como medida de seguridad"*. Agrega Gustavo Sain: *"Fue justamente durante esta época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados Unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial."*[44]

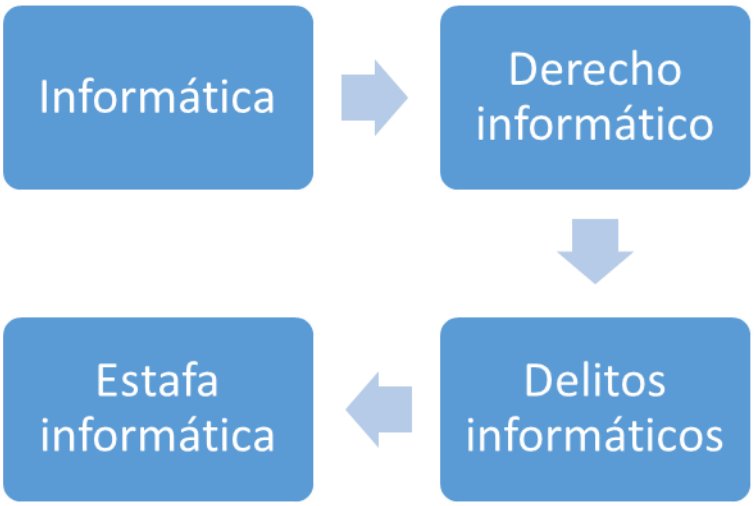
---

[43] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 53.

[44] SAIN, Gustavo. *La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas más allá de la solución penal*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 8.

Para un mejor entendimiento del tema en estudio, haciendo un análisis desde lo general hacia lo particular, debemos definir algunos conceptos trascendentales, con el siguiente orden:

***Gráfico 1**. Antecedentes de la estafa informática*



Por ser los delitos informáticos en términos generales una delincuencia no convencional, así como una producción, manifestación o consecuencia originada de la misma informática, se debe definir en primera instancia qué se entiende por informática, sea: *"Denominación de la técnica informática basada en el rigor lógico y en la automatización posible, al punto de utilizar con frecuencia, y dentro de las posibilidades, las computadoras. Se diversifica en diferentes especies: a) metodológica, que elabora los métodos de programación y exploración de computadoras; b) formal o analítica, que busca los algoritmos más adecuados para la información; c) sistemática o lógica, que estudia la estructura de los sistemas, el funcionamiento de las computadoras y las actividades operativas; d) física o tecnológica, que analiza los componentes físicos que intervienen en los sistemas informativos; e) aplicada, que determina las áreas en las que ha de desenvolverse el procesamiento automático establecido."*[45] La informática *"…constituye el tratamiento automático y racional de la información considerada*

[45] CABALLENAS DE TORRES, Guillermo. *Diccionario de Ciencias Jurídicas*. Editorial Heliasta, 2ª ed. Buenos Aires, 2012, p. 486.

como el soporte de los conocimientos y las comunicaciones. Tiene su origen en el término francés informatique, que se forma, a su vez, del inglés information (información) y del francés automatique (automática); es decir, información automática…"[46]

La informática es una ciencia o disciplina que tiene tareas, tales como: estudiar las funciones de los programas; complejidad de los algoritmos; almacenamiento y organización de datos; la comunicación entre programas y seres humanos (interfaces de usuario y lenguajes de programación)[47]; estudia métodos (proceso y técnicas), con el fin de almacenar, procesar y trasmitir información y datos en formato digital[48]. De conformidad con lo anterior, se determina que la informática pretende ser una herramienta de ayuda para el ser humano en sus labores diarias, acelerando la obtención de información, resultados, solucionando problemas y facilitando trámites.

Por su parte, el "derecho informático" se define *"como el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática"*[49]. Ahora bien ¿qué se debe entender entonces por "delitos informáticos"?[50] Se dice que son aquellos que involucran en su ámbito

---

[46] CEDANO OLVERA, Marco Alfredo, CEDANO RODRÍGUEZ, José Antonio, RUBIO GONZÁLEZ, José Antonio, y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010, p. 3.

[47] CEDANO OLVERA, Marco Alfredo, CEDANO RODRÍGUEZ, José Antonio, RUBIO GONZÁLEZ, José Antonio, y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010, p. 3.

[48] S. MARTÍNEZ, Matilde. *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 34.

[49] S. MARTÍNEZ, Matilde. *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 34.

[50] SAIN, Gustavo. *La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas más allá de la solución penal*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, pp. 9-10: *"¿Pero qué son los delitos informáticos? Si bien no existe una definición específica,*

de acción, variadas conductas con características particulares, las cuales recaen en bienes jurídicos diversos, y que, debido a la relación que tienen con computadores, se les considera dentro de la esfera de delitos informáticos; al ser abstracta la definición, provoca que para los intereses del derecho penal, devenga en un concepto vacío, y es por ello que ese contenido propio, solamente se puede adquirir con una descripción concreta de las conductas que se pretenden castigar[51]. No se puede invisibilizar que la informática es una ciencia con un lenguaje propio, a lo cual se le agrega que es sumamente reciente en la historia de la humanidad y hasta hace pocos años se adoptó dentro del mundo del derecho. Esas circunstancias, entre otras, se consideran para afirmar que los delitos informáticos integran parte de la delincuencia no convencional. Es un hecho indubitable que para el entendimiento de los delitos informáticos se requiere, desde el punto de vista de las personas profesionales en derecho, explorar otra rama del saber, tal y como lo es la "Informática".

La Organización para la Cooperación Económica y el Desarrollo (OCED) define delito informático como *"Cualquier conducta ilegal, no ética, o no autorizada*

---

desde la década de 1970 se esbozaron distintas acepciones en cuanto al alcance del término. Según el Manual de recursos de justicia criminal elaborado por el Departamento de Justicia de los Estados Unidos en 1979, se entienden por estas conductas "cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución. Según una definición brindada por la Organización de Cooperación y Desarrollo Económico, en 1983, el delito informático es "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos". Para el Consejo de Europa, según una definición de 1995, "es cualquier delito penal donde las autoridades de investigación deben obtener acceso a información que ha sido procesada o transmitida por sistemas computacionales o sistemas de procesamiento electrónico de datos". Para el criminólogo Majid Yar, la ausencia de una definición específica sobre el fenómeno del cibercrimen se debe fundamentalmente a que "la delincuencia informática se refiere no tanto a un único tipo distintivo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que tienen en común solamente el medio electrónico (ciberespacio) en el que tiene lugar […] cuando hablamos de delitos informáticos nos referimos a aquellas conductas indebidas e ilegales, en las que interviene un dispositivo informático como medio para cometer un delito o como fin u objeto de este. En este sentido, los delitos informáticos son entendidos según el lugar que ocupa la tecnología en la comisión del delito más que según la naturaleza delictiva del acto mismo..."

[51] G. SALT, Marcos. *Delitos informáticos de carácter económico.* En revista: Delitos no convencionales. Editores del Puerto s.r.l, Buenos Aires, 1994, p. 226.

que involucra el procesamiento automático de datos y/o la transmisión de datos".[52] Asimismo, el autor Miguel Á. Davara Rodríguez, citado por Marcelo Temperini lo define como: *"la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático*[53]*, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software […] Nos estamos refiriendo solamente a la comisión de un delito por medios informáticos o telemáticos, ya que la comisión de otros delitos en los que de alguna forma interviene un elemento informático, se encontrará sin duda dentro del Derecho Penal general."*[54]

Existen varias clasificaciones de los delitos informáticos: los económicos y por otro lado, los encaminados a atacar la privacidad de las personas; en cuanto a los primeros, se consideran las acciones humanas que utilizan un sistema informático[55] como instrumento o tomando al propio sistema como objeto de la

---

[52] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 54.

[53] Ver CEDANO OLVERA, Marco Alfredo, CEDANO RODRÍGUEZ, José Antonio, RUBIO GONZÁLEZ, José Antonio, y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010, p. 4*: "**Telemática** es el término que se utiliza más comúnmente para definir al conjunto de técnicas y servicios que asocian las telecomunicaciones y la informática; sin embargo, ésta también puede definirse como la transferencia de datos a distancia entre y por medio de computadoras, aunque ésta no resulta tan clara en la expresión misma de telemática y menos aún en la amplitud de su aplicación en otras áreas del conocimiento. De esta forma, si sustituimos la palabra transferencia por el concepto de comunicación, será más fácil comprender el término datos con un juicio más amplio y será posible detectar que tras los equipos informáticos se hallan los seres humanos; con base en estas precisiones, la expresión telemática adquiere un significado más completo: "comunicación entre individuos utilizando a la computadora como medio" [...] al referirse al proceso de comunicación, se estará haciendo referencia a los elementos básicos de éste: el mensaje, elaborado por el emisor, se transmite al receptor a través de una computadora y de la línea telefónica o de la red, lo cual se realiza convirtiendo la señal a través de la utilización de un código permitido (programas de comunicación, navegadores, etcétera)."*

[54] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 54.

[55] Ver BÉHAR QUIÑONES, Gastón y YÁÑEZ FIGUEROA, Agustín. *Introducción a los contratos tecnológicos*. Editorial Tecnológica de Costa Rica, 1ª ed. Cartago, 2017, p. 56*: "...los sistemas informáticos son aquellas plataformas tecnológicas que administran la información de acuerdo con las instrucciones que brinda el código fuente y que son entendidos o conceptualizados como funcionalidad. Estos sistemas informáticos pueden ser creados dentro del hardware o por medio de*

conducta disvaliosa (se puede atacar el Hardware o el Software[56]), tienen además una repercusión patrimonial; los segundos, son los dirigidos a afectar el ámbito privado de los ciudadanos, ya sea mediante la acumulación o la difusión de datos los cuales están contenidos en un sistema informático (se puede atacar el patrimonio, la privacidad o la seguridad supraindividual)[57] [58]; a la luz de la descripción objetiva del numeral 217 bis del CP, podríamos afirmar, tal y como se analizará más adelante, que, la estafa informática contiene ambos matices, por ser un tipo penal pluriofensivo.

En la literatura se habla de "delito informático" y en ocasiones de "cibercrimen", en ese sentido, para una mejor precisión de los conceptos, nos remitimos a lo dicho por el autor Marcelo Temperini, quien considera que la "organización del delito" (que no es otra cosa más que el plan de autor y la distribución de funciones en los delitos cometidos en coautoría) es lo que distingue el concepto de cibercrimen del delito informático. Establece que "delito informático" es aquel que es cotidiano, ocurre de modo independiente y aislado, sin que se cuente con indicios que hagan presumir que se está ante una organización delictiva; mientras tanto al "cibercrimen", lo considera como una serie de delitos informáticos, con mayor grado de profesionalismo y estructura, con motivaciones

---

espacios virtuales, y son accesibles desde diversos sistemas de tecnología sin mayores restricciones materiales o espaciales que aquellas delimitadas por las partes y por la propia tecnología…"

[56] Ver BÉHAR QUIÑONES, Gastón y YÁÑEZ FIGUEROA, Agustín. *Introducción a los contratos tecnológicos*. Editorial Tecnológica de Costa Rica, 1ª ed. Cartago, 2017, p. 36*: "...el software, en su expresión más simple, es un ordenador de información que, segmentado en bases de datos, ayuda a las personas a tomar decisiones informadas de una manera más efectiva y ejecutiva. Esta es la razón principal por la que una organización adquiere un software, pero en este proceso de adquisición o puesta en marcha (go live) intervienen muchas entidades que se involucran en su definición, desarrollo, implementación y mantenimiento. Todas estas entidades tienen diferentes personas trabajando para ellas, cuyos intereses difieren a la hora de desarrollar o instalar un software. La empresa proveedora de bienes y servicios tecnológicos tiene una expectativa diferente de aquélla que busca adquirirlo y esta, a su vez, otra muy distinta a la del equipo que está instalando el software…"*

[57] G. SALT, Marcos. *Delitos informáticos de carácter económico.* En revista: Delitos no convencionales. Editores del Puerto s.r.l, Buenos Aires, 1994, p. 227.

[58] LUZ CLARA, Bibiana. *Manuel de derecho informático*. Editorial Jurídica NOVA TESIS, Argentina, 2001, p. 118.

económicas, señala como ejemplo: Los sujetos activos que conforman un grupo para realizar estafas electrónicas, captan de manera ilegítima datos confidenciales, información pescada (phishing[59]), como nombres de personas usuarias, contraseñas y detalles de tarjetas bancarias, lo cual implica simular ser un contacto confiable y legítimo. En la estructura de la organización, se cuenta con diseñadores de páginas mellizas (que engañan a la víctima); encargados de la distribución vía engaño; encargados de recolectar los datos y procesarlos; quienes realizan las estafas con ardid o engaño y un perjuicio económico; así como encargados de blanquear el dinero, entre otros.[60]

Vale mencionar que el profesor Francisco Castillo, considera que el concepto de criminalidad por computadora tiene dos connotaciones[61]:

Tabla 1. Connotaciones de la criminalidad por computadora

En sentido amplio	*"…cualquier delito convencional, en el cual la computadora es un medio para hacer más eficiente la ejecución del hecho, de tal modo que **el sistema informático constituye solamente el medio de comisión de la infracción**. En tales casos, la Internet no es el único medio de comisión del delito, sino que*

[59] ORGANISMO DE INVESTIGACIÓN JUDICIAL. SECCIÓN DE DELITOS INFORMÁTICOS. *Folleto delitos informáticos*. Versión electrónica en: https://sitiooij.poder-judicial.go.cr/images/folletos/delitos%20informaticos.pdf: *"**¿Qué es phishing?** Es una estafa o fraude que utilizando medios informáticos o electrónicos e ingeniería social, tiene como fin extraer información confidencial de sus victimas (sic) y utilizarla para extraer dinero u otros fines. Para esto se hace pasar por una persona o empresa que requiere su información confidencial, tal como: • Número de Tarjetas de debito (sic) o crédito • Contraseñas o claves de paso • Información de cuentas • Información personal. La víctima puede ser abordada mediante: • SMS (mensaje de texto) • Llamada telefónica • Página de Internet o ventana emergente h t t p : / / w w w . n o m b r e d e l b a n c o paginasgratis.com • Correo electrónico. **Características**: • Los correos electrónicos parecen ser enviados por una cuenta de correo electrónico real del banco, empresa o inclusive persona real. agenciavirtual@banco.fi.cr. • Factor miedo, con el fin de conseguir una respuesta inmediata de la víctima. Amenaza a la víctima con perder dinero o cerrar la cuenta sino sigue las instrucciones del correo electrónico. • El correo electrónico incluye un acceso directo o vínculo o link, supuestamente a la página de Internet del banco. http://www. nombredelbanco.paginasgratis.com/. • Creación de una página de Internet casi igual a la de la entidad bancaria o empresa. • En ella se pide la información confidencial de la víctima."*

[60] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, pp. 56-57.

[61] CASTILLO GONZÁLEZ, Francisco. *El delito de estafa*. Editorial Jurídica Continental, San José, 2ª ed. 2013, pp. 44-47.

	ellas son un medio de comunicación […] Algunos, como Müller (Jérémie), consideran que a este grupo pertenece la estafa común en la que el agente se ayuda por medio de la Internet para cometerla. ***En todo caso, no es la situación con la estafa informática (art. 217 bis Cód. pen.), en la cual se utiliza, de manera esencial, un sistema informático para realizarla****. En estos casos enumerados, la red no es ni el lugar en que los delitos son cometidos ni es el instrumento de la comisión del hecho****. La red es simplemente un medio de comunicación como podría serlo el correo tradicional, la prensa o el teléfono…"* (el resaltado y subrayado no corresponden al original)
En sentido estricto	*"…se considera que la criminalidad por computadora se caracteriza porque en el acontecimiento general* ***juega un papel central un sistema automatizado de procesamiento de datos como medio de comisión o como objeto material de la acción*** *[…] Internet es óptima como instrumento de comisión del delito cuando se trata de delitos que involucran la toma, la destrucción, el borrado o el intercambio de informaciones, datos y programas […] A este grupo pertenecen los siguientes grupos de delitos […] (3) La manipulación de computadora o el uso de datos sin permiso del derecho-habiente, que cubre la estafa informática (art. 217 bis Cód pen.)…"*

De igual manera, tal y como lo habíamos indicado párrafos atrás, la delincuencia informática puede ser considerada como no convencional, ya que *"...es posible decir que, en verdad, no se trata, propiamente, de hechos punibles "no comunes" o "no tradicionales", sino que se trata, antes bien, por un lado, de nuevas formas de comisión de los hechos punibles de siempre o, por el otro lado, de* ***la utilización de nueva tecnología, de nuevos instrumentos, para cometer delitos que podríamos llamar clásicos. Así, puede entrar en el catálogo también la problemática de los delitos llamados "delitos informáticos".*** *Empero, un hilo conductor que nos permita contener en un mismo conjunto –el de los "delitos no convencionales"- hechos que afectan distintos bienes jurídicos y de modo diverso, se debe construir a partir de un denominador común: el enorme daño social, concreto o potencial (recuérdese que las figuras en cuestión se presentan mayoritariamente como delitos de peligro, incluso abstracto) que estas*

acciones acarrean para el desarrollo político, económico, social y cultural de la población afectada…"[62]

En ese mismo orden de ideas, el Dr. Altmark citado por Matilde S. Martínez, indica con respecto a la delincuencia informática que *"se trata de conductas antijurídicas no tan ordinarias, pues suponen un mínimo de conocimientos y de acceso a la tecnología, que se realizan a partir de un sistema, utilizando a este como un instrumento eficaz para lograr el objetivo delictivo perseguido,* ***ya sea manipulando el soporte lógico de aquel, o bien utilizando ilegítimamente los datos y programas de un sistema****, o bien utilizando correctamente el sistema pero para introducirse en otro y otros y producir un resultado disvalioso en bienes económicos o personales de otros sujetos..."*[63] En un plano eminentemente teórico, los delitos informáticos son delincuencia no convencional, sin embargo, es importante analizar mediante casos concretos, cuáles son las conductas que, en Costa Rica, han sido procesadas y sancionadas como estafas informáticas, es decir, desde un enfoque empírico, situación que se analizará en el último capítulo de esta investigación.

Para abordar el concepto de estafa informática y como un antecedente, se debe mencionar que Costa Rica mediante la Ley N° 9452 del 26 de mayo de 2017, publicada en el Alcance N° 171 de la Gaceta Digital N° 125 del 03 de julio de 2017, con entrada en vigencia el 01 de enero de 2018, se adhirió al Convenio sobre la Ciberdelincuencia, desarrollado en Budapest, el 23 de noviembre de 2001, con entrada en vigencia el 01 de julio de 2004. Con respecto al tema que nos ocupa, dicho Convenio Internacional trata la figura que, en Costa Rica denominamos "estafa informática", como "fraude informático", indicando el Convenio en el artículo N° 8 lo siguiente: *"****Fraude informático****. Cada Parte*

---

[62] R. PASTOR, Daniel. *¿Es conveniente la aplicación del proceso penal "convencional" a los delitos no "convencionales"?* En revista: Delitos no convencionales. Editores del Puerto s.r.l., Buenos Aires, 1994, pp. 272-273. El resaltado no corresponde al original.

[63] S. MARTÍNEZ, Matilde. *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 34. El resaltado no corresponde al original.

adoptará las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, los actos deliberados e ilegítimos que ***causen perjuicio patrimonial*** *a otra persona mediante: a)* ***cualquier introducción, alteración, borrado o supresión de datos informáticos****; b)* ***cualquier interferencia en el funcionamiento de un sistema informático****, con la intención, fraudulenta o delictiva, de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona."*[64] Es claro que la sugerencia, a pesar de permitir a los Estados parte un amplio margen de actuación, sí delimitó que el interés era proteger únicamente el bien jurídico patrimonio, y que el delito se denominaría "fraude informático" (esos extremos son trascendentes para el presente trabajo, siendo analizados posteriormente a la luz de la redacción del numeral 217 bis del CP). Es decir, después del Convenio sobre Ciberdelincuencia de Budapest, transcurrieron 13 años para que Costa Rica se adhiriera al mismo, pero ya para ese momento nuestro ordenamiento jurídico-penal había sufrido las siguientes variaciones con respecto a dicho delito informático: **1)** Había contemplado el delito denominado "fraude informático" en el artículo 217 bis del CP, mediante Ley N° 8148 del 24 de octubre de 2001, publicada en La Gaceta el 21 de noviembre de 2001[65], es decir, anterior al mismo Convenio que se desarrolló el 23 de noviembre de 2001; **2)** Reformó el numeral 217 bis del CP, denominando el delito como "estafa informática", mediante Ley Nº 9048 del 10 de julio de 2012, publicada en el Alcance Nº 172 de La Gaceta Nº 214 del 06 de noviembre de 2012.

Se ha entendido que la estafa informática, se puede cometer de diferentes formas, entre otras, las siguientes: *"…podríamos decir que el "phishing" es la pesca de datos personales a través de Internet. Ahora bien, ella puede constituir una modalidad de estafa informática, si tiene lugar a través del envío masivo de*

[64] El resaltado no corresponde al original.

[65] Ver análisis del expediente legislativo N° 14097 en el que se incluyó el delito de "fraude informático", en: LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 1ª ed. San José, 2011, pp. 103-131.

correos electrónicos con enlaces a páginas "web" falsas, respecto de las cuales se imita el contenido o la imagen de un determinada entidad financiera o bancaria para engañar al destinatario del mensaje, logrando así sustraer la información personal que posibilita el acceso a sus cuentas de débito personal. De este modo, se logra la consumación de un perjuicio patrimonial mediante el retiro de dinero, o bien, directamente a través de operaciones de compras no consentidas por Internet. A su turno, el "pharming" consiste, según se ha esbozado, en la manipulación técnica de las direcciones DNS que son utilizadas por un determinado usuario, reconduciendo la navegación que este realiza a sitios "web" que presentan un aspecto idéntico, pero que son falsos y han sido creados "con fines defraudatorios". Esta figura puede operar como modalidad de estafa informática si con el mecanismo indicado se consigue la cesión de datos personales financieros o bancarios, con el propósito ulterior de realización de ilícitos de apoderamiento patrimonial de dinero o activos en cuentas corrientes. Finalmente, con los anglicismos "money-mules", "phishing-mules" o "pharming-mules", se hace referencia a una conducta de colaboración que opera con posterioridad a la consumación de la defraudación patrimonial. Ella consiste, esencialmente, en poner a disposición de los estafadores ("scammers") los dineros obtenidos por éstos a través del "phishing" o "pharming". Generalmente, la mula informática pacta con los estafadores una comisión que asciende a la décima parte de las transferencias de origen ilícito. Así, una vez que ha operado el acuerdo y se ha consumado la defraudación, procede al giro de los dineros depositados por los estafadores o "scammers" en sus cuentas de los muleros, que sirven como blanqueadores o lavadores de los montos defraudados en el territorio nacional, en cuanto realizan, posteriormente, las remesas de dichos fondos al extranjero utilizando para ello las casas de cambio establecidas, empresas de paquetería postal y las que ofrecen envíos de dineros al exterior."[66]

---

[66] OXMAN, Nicolás. *Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"*. En: Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, N° 41, Valparaíso, 2013. Versión electrónica en: http://www.scielo.cl/scielo.php?pid=S0718-68512013000200007&script=sci_arttext.

De acuerdo con lo anterior, ya sea la estafa informática o el fraude informático, terminan siendo delitos en los que se puede incurrir de distintas formas, sin embargo, teóricamente, siempre están dirigidos a lesionar el patrimonio ajeno. Es importante aclarar que, hasta el momento no se ha abordado en la investigación, conforme al principio de legalidad, la literalidad del numeral 217 bis del CP, como para afirmar fehacientemente: 1) que sea el patrimonio el único bien jurídico tutelado en dicho numeral y 2) que nos encontremos ante una verdadera estafa. Recuérdese que una cosa es la teoría, y otra, lo que sucede en la realidad, tal y como refiere el autor Guillermo Cabanellas: *"El legislador puede ordenar que a la vaca se la llame oveja; lo que no puede lograr es que le crezca lana."*[67] Precisamente por esa razón, en el siguiente capítulo se abordarán las figuras penales de la estafa general y la estafa informática, ahondándose aún más el estudio de esta última.

Capítulo II. Comparación entre estafa general y estafa informática

Para una aproximación más certera al delito que nos ocupa, debemos recurrir a un análisis secuencial terminológico, consistente en primera instancia, en precisar qué se entiende por la acción de estafar, ejercicio que en tesis de principio debería ser útil para el siguiente paso, el cual consistirá no sólo en buscar qué se entiende por estafa informática, sino en contrastarlo con la estafa general. Nótese que por un asunto meramente semántico, al denominarse ambos tipos penales como “estafas”, deberían contener por lógica y de acuerdo con la armonía de nuestro ordenamiento jurídico, algunas similitudes entre sí[68]. Entonces, cabe

---

[67] CABANELLAS DE LAS CUEVAS, Guillermo. *Propiedad intelectual sobre los programas de computación*. Heliasta, 1ª ed. Buenos Aires, 2011, p. 19.

[68] GARCÍA FIGUEROA, Alfonso; GASCÓN ABELLÁN, Marina; MARCILLA CÓRDOBA, Gema; PRIETO SANCHÍS, LUIS. *Argumentación jurídica*. Tirant lo Blanch. Valencia. 2014, pp. 257-259: *“(a) Interpretación gramatical (o literal): consiste en atribuir significado a una disposición teniendo en cuenta la semántica, la sintáctica y la pragmática de la lengua en que tal disposición se expresa […] i) El principal argumento que sirve a la interpretación declarativa se denomina argumento del lenguaje común, según el cual una disposición debe ser interpretada según el significado ordinario de las palabras y las reglas gramaticales de la lengua comúnmente aceptadas. Conviene observar sin embargo, que el significado ordinario de las palabras con frecuencia padece —como vimos en el tema anterior— de ambigüedad y vaguedad, por lo que puede resultar controvertido. De manera*

preguntarse ¿Tendrán la estafa general y la estafa informática similitudes entre sí? o ¿Estaremos ante tipos penales completamente distintos? Una vez conceptualizado qué se debe entender por la acción de estafar, se procederá con la respectiva comparación entre este tipo penal previsto en el artículo 216 del CP y la estafa informática, regulada en el 217 bis del mismo cuerpo legal, para así visibilizar si existen o no similitudes o diferencias.

Estafa general

Según el Diccionario de la Real Academia Española (DRAE), el verbo infinitivo "estafar" se define como: *"1. tr. Pedir o sacar dinero o cosas de valor con artificios y engaños, y con ánimo de no pagar. 2. Der. Cometer alguno de los delitos que se caracterizan por el lucro como fin y el engaño o abuso de confianza como medio."* Para la investigación, en primera instancia nos interesa la segunda acepción, correspondiente a "Derecho", resaltando que para estafar se requiere una conducta realizada con engaño o abuso de confianza. En ese mismo sentido, el DRAE define el término "estafa" como *"Der. Delito consistente en provocar un perjuicio patrimonial a alguien mediante* ***engaño y con ánimo de lucro****."*[69]

El Diccionario de Ciencias Jurídicas, Cabanellas de Torres, define el concepto de "estafa" como: *"Delito genérico de defraudación que se configura por el hecho de causar a otro un perjuicio patrimonial, valiéndose de cualquier ardid o*

---

que el argumento del lenguaje común, que sin duda ha de ser el primero de los argumentos interpretativos, no es siempre resolutivo. (b) Interpretación sistemática: consiste en atribuir significado a una disposición contextualizándola en un sector del ordenamiento o en el ordenamiento en su conjunto […] i) Argumento de la sedes materiae: una disposición debe interpretarse de un cierto modo y no de otro en virtud de su colocación en el contexto normativo del que forma parte. Se piensa, en definitiva, que la localización topográfica de una disposición proporciona información sobre su significado, pues se presume que el legislador racional ordena lógicamente las materias tratadas. Muy relacionado con este argumento está el argumento a rubrica: una disposición debe ser interpretada considerando el título o rúbrica que encabeza el grupo de disposiciones en el que se inserta. ii) Argumento de la constancia terminológica: ha de entenderse que el legislador emplea los vocablos con un significado constante, al menos dentro del mismo texto legal. iii) Argumento económico (o no redundancia): cuando quepa atribuir más de un significado a una disposición, han de rechazarse aquéllos que supongan una reiteración de lo establecido por otra disposición. Remite, pues, a la idea de un legislador racional que sigue criterios de economía y no repetición…"

[69] El resaltado no corresponde al original.

engaño, tales como el uso de nombre supuesto, de calidad simulada, falsos títulos, influencia mentida, abuso de confianza o ficción de bienes, créditos, comisión, empresa o negociación. Delitos específicos de estafa están representados por otros casos especiales de defraudación."[70] En cuanto al verbo "estafar", lo conceptualiza de la siguiente manera: *"Estrictamente, cometer una estafa (v.). | Engañar. | Defraudar. | Obtener dinero u otros bienes muebles sorprendiendo la buena fe de quien los posee. | Faltar a la palabra; no cumplir lo prometido."*[71]

Por su parte el verbo defraudar, el DRAE lo define como: *"1. tr. Privar a alguien, con abuso de su confianza o con infidelidad a las obligaciones propias, de lo que le toca de derecho. 2. tr. Frustrar, desvanecer la confianza o la esperanza que se ponía en alguien o en algo. 3. tr. Eludir o burlar el pago de los impuestos o contribuciones. 4. tr. Turbar, quitar, entorpecer algo."* De esas definiciones, se desprenden elementos importantes, tales como que la estafa en sentido estricto se entiende como un delito de defraudación, en el cual el sujeto activo realiza necesariamente un comportamiento caracterizado por ser engañoso o con un ardid. Sin embargo, en sentido amplio, se deja abierta la posibilidad de que se estafe mediante una "defraudación", en la cual podríamos incorporar comportamientos que no necesariamente incluyan el ardid o engaño, como cuando se turba, se quita o se entorpece algo. Ahora bien, por la rama del derecho en la que nos desenvolvemos, es necesario restringir el concepto, siendo que, al unísono, siempre se ha entendido en sentido jurídico-penal, la acción de estafar como un ardid o un engaño en que se hace incurrir al sujeto pasivo.

Ante la evolución del entorno y las realidades cambiantes en las que se desenvuelven las personas, la figura de la estafa ha sufrido variaciones. La presente investigación no pretende abordar ese desarrollo evolutivo por completo, ya que sería irrelevante para el trabajo, lo que sí resulta significativo es el

---

[70] CABALLENAS DE TORRES, Guillermo. *Diccionario de Ciencias Jurídicas*. Editorial Heliasta, 2ª ed. Buenos Aires, 2012, p. 379.

[71] CABALLENAS DE TORRES, Guillermo. *Diccionario de Ciencias Jurídicas*. Editorial Heliasta, 2ª ed. Buenos Aires, 2012, p. 379.

desarrollo conceptual del delito de estafa básica en Costa Rica. De esa manera, deviene útil y necesario, hacer un breve recuento histórico del fenómeno criminal de la estafa y su respectivo tratamiento en la legislación costarricense.

Desde el CP de 1841 (Código General de Carrillo) en el Título III se contemplaba un Capítulo denominado *"De las estafas y engaños"*, integrado por siete delitos, entre los cuales se encontraba el numeral 637, y que definía la estafa[72] como: *"Cualquiera que con algún artificio, engaño, superchería, práctica supersticiosa y otro embuste semejante, hubiere sonsacado a otro dineros, efectos o escrituras o le hubiere perjudicado de otra manera en sus bienes, sin alguna circunstancia que lo constituya verdadero ladrón, falsario o reo de otro delito especial, sufrirá pena de reclusión por el tiempo de un mes a dos años y una multa de diez a cien pesos, sin perjuicio de la pena mayor que merezca como ladrón, falsario o reo de otro delito, si justamente lo fuere".* El artículo transcrito de acuerdo al profesor Francisco Castillo González, proviene del numeral 766 del CP español de 1822, y éste tiene su origen en el artículo 430 del CP francés de 1810 (Código de Napoleón).[73]

Si se observa el numeral 637 del CP de 1841 se desprenden las siguientes características: *"(1) De la utilización de "algún artificio, engaño, superchería, práctica supersticiosa y otro embuste semejante", podemos concluir que no basta para constituir estafa la simple mentira, sino que se requiere una mentira calificada. (2) Este artificio, engaño, etc. debe haber engañado al sujeto pasivo. El engaño sobre el sujeto pasivo se indica con el verbo "sonsacar" "a otro". (3) El objeto material del acto dispositivo del ofendido se indica en el texto del artículo 637 como "dineros, efectos o escrituras" o "…en sus bienes". (4) De acuerdo al artículo 637 del Código de Carrillo se requiere un acto dispositivo del engañado. (5) Por último, la estafa prevista en el artículo 637 del Código de Carrillo requiere*

[72] CASTILLO GONZÁLEZ, Francisco. *El delito de estafa*. Editorial Jurídica Continental, San José, 2ª ed. 2013. p. 35.

[73] CASTILLO GONZÁLEZ, Francisco. *El delito de estafa*. Editorial Jurídica Continental, San José, 2ª ed. 2013. p. 35.

un perjuicio económico, que se indica con la frase: "le hubiere perjudicado de otra manera en sus bienes".[74]

Se deriva entonces que, la estafa aplica cuando se defraude a una persona física por medio de un ardid o de un engaño. En realidad se puede decir que los conceptos de ardid, engaño o timo son sinónimos, y configuran el elemento esencial de la estafa para engañar al ofendido a que entregue la cosa, el derecho o el bien al estafador.[75]

El profesor Francisco Castillo, intervino para la modificación del actual numeral 216 del CP, que se lee de la siguiente manera: *"Quien, induciendo a error a otra persona o manteniéndola en él, por medio de la simulación de hechos falsos o por medio de la deformación o el ocultamiento de hechos verdaderos, utilizándolos para obtener un beneficio patrimonial antijurídico para sí o para un tercero, lesione el patrimonio ajeno, será sancionado de la siguiente forma…"* Con dicha reforma según el profesor Castillo, se varió el objeto de protección en este tipo de delitos, se pasó de la estafa como delito contra la propiedad, a la estafa como delito contra el patrimonio. De esa manera, las reformas de 1988 y 1993, variaron de forma radical las características del delito de estafa, entre ellas el tipo objetivo y a nivel de la penalidad.

Esta breve reseña histórica, es útil para delimitar que por estafa se ha entendido (por lo menos antes de la redacción de la estafa informática) la acción humana del sujeto activo dirigida en contra de una persona física (estafado o estafada), a quien se le induce a error como consecuencia del ardid o del engaño (nexo de causalidad), precisamente esas acciones fraudulentas se convierten en requisitos indispensables del delito de estafa, tal y como se refiere a continuación: *"…El elemento neurálgico y central del delito de estafa es el engaño o conducta engañosa, que según la redacción del tipo básico debe ser bastante, es decir,*

---

[74] CASTILLO GONZÁLEZ, Francisco. *El delito de estafa*. Editorial Jurídica Continental, San José, 2ª ed. 2013. p. 36.

[75] CASTILLO GONZÁLEZ, Francisco. *El delito de estafa*. Editorial Jurídica Continental, San José, 2ª ed. 2013, pp. 39-40.

idóneo – tanto desde un prisma objetivo como subjetivo– para producir error a otra u otras personas. El siguiente eslabón de la cadena típica y lógica del delito de estafa lo constituye el error, situación de discordancia entre la representación de la realidad por parte de quien sufre el engaño y los hechos efectivos del mundo exterior, provocada por el sujeto activo mediante la conducta engañosa. En la continuación de los hechos típicos desarrollados por el autor aparece la producción de un acto de disposición patrimonial, consecuencia a su vez de la situación de error..." [76]

En armonía con lo anterior, y para un análisis de la figura de estafa general, debemos recordar que *"De acuerdo a la opinión mayoritaria la inducción en error implica que el comportamiento del autor produzca en el engañado una falsa representación que antes de la acción del agente no existía o no existía en la forma en que éste la produjo en la cabeza del engañado. Engañar significa, según la doctrina dominante, causar una equivocación en la representación de la víctima. El engaño no contiene ningún elemento subjetivo. La doctrina dominante define el engaño de manera estrictamente objetiva: engaño es cualquier comportamiento que de manera objetiva conduzca a la víctima al error o que la mantenga en él y que, por ello mismo, influya en la representación de la víctima. "Comportamiento engañoso" significa que hay engaño en donde ocurra fácticamente la conducción a engaño, es decir, en donde hay una pretensión de hechos del autor que no corresponde con la realidad o que, correspondiendo y siendo verdadera, se la utiliza como medio de engaño y es causal para la representación errónea del engañado […] En lugar de la clasificación legal de las formas de engaño (simulación de hechos falsos, deformación u ocultamiento de hechos verdaderos), que hoy día se ha reconocido como inservible, se ha establecido en la doctrina*

[76] JAVATO MARTÍN, Antonio Mª. *Sobre: "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"*. En: Revista Electrónica de Ciencia Penal y Criminología. N° 10-r5, ISSN 1695-0194, 2008, p. 2. Versión electrónica en: http://criminet.ugr.es/recpc/10/recpc10-r5.pdf.

una división del concepto de engaño que lo distingue en modalidades: el engaño explícito, el engaño concluyente y el engaño por omisión de aclaración."[77]

En virtud de todo lo anterior, la única forma de estafar a una persona en sentido jurídico penal, es mediante un ardid o engaño, de tal manera que se le induce a error, para que tome una disposición patrimonial en su perjuicio o de un tercero, *"si no hay ardid o engaño, aunque exista error y disposición patrimonial perjudicial, debe descartarse categóricamente el delito"*.[78]

Ahora bien, analizado a grandes rasgos el delito de estafa general, damos paso al estudio sobre qué se entiende en nuestro ordenamiento jurídico por estafa informática, según el artículo 217 bis del Código Penal.

Estafa informática

La estafa informática a diferencia de la estafa base, nace en una coyuntura muy reciente de la historia de la humanidad, propiamente en la sociedad moderna de la globalización, en la que las personas tecnológicas, dominan la información y la comunicación, pero de forma computarizada, circunstancia aprovechada por sujetos para lesionar el patrimonio de otros seres humanos.

Asimismo, atendiendo la secuencia de nuestro CP, no podemos ocultar que la figura de la estafa informática (artículo 217 bis) debería tener algún tipo de correspondencia con la estafa básica (artículo 216), no sólo porque ambas fueron denominadas "estafas" por las personas legisladoras, sino, además, porque se ubican dentro del *"Título VII. Delitos contra la propiedad"*, *"Sección IV. Estafas y otras defraudaciones"*.

Ahora bien, es necesario confrontar con el delito de estafa general, el tipo penal de estafa informática prevista y sancionada en el artículo 217 bis del CP,

---

[77] CASTILLO GONZÁLEZ, Francisco. *El delito de estafa*. Editorial Jurídica Continental, San José, 2ª ed. 2013, pp. 146, 147 y 149.

[78] DONNA, Edgardo Alberto y DE LA FUENTE, Javier Esteban. *Aspectos generales del tipo penal de estafa*. En: Revista Latinoamericana de Derecho, año I, N° 1, 2004, p. 49.

con vigencia desde el 06 de noviembre de 2012, el cual se lee de la siguiente manera:

"Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos."

Como punto de partida, podríamos cuestionarnos: ¿Describe realmente esa redacción una estafa tal y como se ha entendido? ¿Sigue la estafa informática las mismas reglas que la estafa base? Para encontrar respuestas a esas interrogantes, el jurista Francisco Castillo mencionó: *"…En la estafa informática no existe ni un engaño ni una víctima de un engaño. De modo que suponer un error es una ficción y con ello se llega a una analogía prohibida en perjuicio del reo. Los elementos de engaño de la estafa general (art. 216 Cód. Pen.) no pueden corresponder a la estafa informática (art. 217 bis Cód. Pen.), pues esta última figura tiene elementos de la administración fraudulenta y hace referencia a los delitos contra la propiedad, lo que se manifiesta en que una de las alternativas de acción punible consiste en el empleo indebido (en contra de la voluntad del derecho-habiente) de datos, cuestión que no ocurre en la estafa general. Por ello, la doctrina mayoritaria no admite un paralelismo entre entre lla (sic) acción de la*

estafa general y la acción de la estafa informática…"[79] Toma trascendental importancia el tema del ardid o del engaño, toda vez que, tal y como se dijo líneas atrás, esa es una característica nuclear de la estafa convencional, pero que se encuentra ausente en la estafa informática, siendo que las computadoras no tienen conciencia por lo tanto no pueden ser sujetas a engaño[80]. En ese sentido se indica sobre las máquinas que *"…Su limitación más importante es que no pueden pensar por sí mismas; es decir, no les es posible resolver problemas ni tomar decisiones sin la intervención del hombre. Su mayor virtud es que son muy útiles en la organización de la información para la resolución de problemas y la toma de decisiones, lo cual es resultado de la programación de los expertos en computación. Las computadoras pueden efectuar cosas sorprendentes siempre y*

[79] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 55.

[80] Programa Televisivo Español "Redes" (dirigido por Eduard Punset) episodio denominado: *"Conciencia y Universo, más allá de la física cuántica"*, año 2006 (secuencia horaria del minuto 01:33 a 03:51). Dirección electrónica: https://youtu.be/_7YVlYt5lKo: *"Hace 10 años la computadora Deep Blue ganó una partida a Kasparov, el campeón mundial de ajedrez. Los defensores de la inteligencia artificial cantaron victoria, por fin quedaba claro que era posible crear computadoras más inteligentes que los humanos, sólo hacía falta disponer de la tecnología necesaria y tener un conocimiento suficiente de las leyes físicas. Hoy tenemos robots que realizan tareas con una rapidez y precisión que superan con mucho a cualquier humano. Los informáticos programan ordenadores cada vez más complejos, el objetivo último es crear un cerebro que tenga cables y chips en vez de neuronas y sinapsis, pero hay algo que se les escapa, un ordenador no siente el frío ni el calor, no se emociona ni comprende las cosas, en definitiva un ordenador no tiene conciencia y sin ella es imposible crear una verdadera inteligencia, a partir de aquí surge una pregunta difícil de responder: ¿de dónde sale la conciencia?, a pesar de que algunos físicos y neurólogos afirman que las leyes que operan en el cerebro son perfectamente conocidas, hay un gran interrogante que se esconde detrás de la conciencia y no es el único, si repasamos la historia de la física veremos que aún quedan bastantes incógnitas por resolver, todavía no se ha logrado hacer totalmente compatible la teoría cuántica con la teoría de la relatividad especial de Einstein, tampoco se comprende la naturaleza del espacio a la escala infinitamente pequeña de las partículas elementales, la conciencia es otra de estas incógnitas, no se puede explicar ni con la mecánica clásica ni con la cuántica, se pueden crear algoritmos para que una computadora sea capaz de realizar cálculos y operaciones muy complicados, pero la naturaleza del pensamiento humano y de los mecanismos de comprensión no es algorítmica y por lo tanto es imposible crear conciencia a partir de datos y ecuaciones. Tiene que haber algo más, algo que explique la emergencia del pensamiento y los sentimientos, la capacidad de tener una idea y de recordar, una ley que opera en nuestro cerebro y que explica la diferencia entre un ser humano y un ordenador capaz de ganarle una partida de ajedrez."*

cuando sigan, paso a paso, las instrucciones de los programas creados por personas, quienes son las que piensan antes de escribir los programas..."[81]

El autor Antonio Mª Javato Martín haciendo referencia a Ricardo Mata y Martín, señala: *"…Llegados a este punto, MATA Y MARTÍN incide en el mantenimiento por la praxis y la literatura española mayoritaria, a imagen y semejanza de lo que acontece en el Derecho comparado, de una noción personalista del engaño propio de la estafa, lo que vendría a justificar la subsunción en ella de todos aquellos supuestos de empleo de medios de pago electrónico que requieran la presencia física o contacto personal de las dos partes de la operación; y a excluir el engaño en conductas dirigidas sobre elementos automáticos…"*[82]

Se encuentra de esa manera la primera diferencia, y esa es que, en la estafa informática no estamos ante un engaño, de la cual derivan otras, ya que, como consecuencia, tampoco existe una persona engañada, lo que implica necesariamente que la estafa informática no es un delito de autolesión, sino que, es de daño ajeno[83]:

Tabla 2. Diferencias entre la estafa general y la estafa informática

Característica del tipo penal	Estafa base (art. 216 del Código Penal)	Estafa informática (art. 217 bis del Código Penal
Engaño o ardid	Sí existe	No existe

[81] CEDANO OLVERA, Marco Alfredo, CEDANO RODRÍGUEZ, José Antonio, RUBIO GONZÁLEZ, José Antonio, y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010, pp. 20-21.

[82] JAVATO MARTÍN, Antonio Mª. *Sobre: "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"*. En: Revista Electrónica de Ciencia Penal y Criminología. N° 10-r5, ISSN 1695-0194. Versión electrónica en: http://criminet.ugr.es/recpc/10/recpc10-r5.pdf, 2008, p. 3.

[83] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 54-56.

Víctima engañada	Sí existe	No existe
Delito de autoengaño o autolesión	Sí	No. Se trata de daño ajeno

De tal forma, las diferencias terminan siendo abismales, ello a pesar de que ambas acciones son denominadas como estafas en el derecho positivo. Para comparar dichos tipos penales, inclusive es necesario acudir a analogías como las siguientes: *"Datos" son, al lado de "informaciones", "programas" y "procesamiento de datos de un sistema automatizado de información", el objeto material de la acción del artículo 217 bis Cód. pen., (estafa informática) así como los "hechos" son el objeto material de la acción en el art. 216 Cód. pen (estafa general)."*[84] Refiere el autor Francisco Castillo que, un dato falso es aquel que contraría la realidad, por lo que existe conexión entre el concepto de "datos falsos" y el de "hecho falsos" de la estafa general.[85] Otra analogía para igualar forzosamente dichos tipos penales es la siguiente: *"El elemento del tipo de causar un resultado en el sistema de procesamiento de datos, como resultado intermedio, es la contrapartida de la producción de un error en la estafa general"*.[86]

Atendiendo el principio de legalidad, podríamos entonces cuestionar si la descripción de la conducta del numeral 217 bis del CP, es coherente con el título del delito, al denominarlo como una especie de "estafa". De conformidad con el

[84] CASTILLO GONZÁLEZ, Francisco. *La estafa informática de "Lege lata" y de "lege ferenda"*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 277.

[85] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 87.

[86] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 111.

DRAE, lo descrito en el tipo penal no encaja en la definición del concepto, ya que, tal y como se expuso párrafos atrás, siempre se consideró que la estafa posee un contenido de engaño o ardid. Si tomamos como ejemplo la primera acepción de estafar según el DRAE, mediante una interpretación literal, evidenciamos que lo descrito en el numeral 217 bis del CP no es una estafa: *"1. tr. Pedir o sacar dinero o cosas de valor con artificios y engaños, y con ánimo de no pagar"*, nótese que se ocupa la existencia siempre del engaño, es decir, la palabra "artificios" no es disyuntiva de "engaños", están separadas por una letra "y" copulativa, es decir que ata ambos conceptos. En cuanto a la segunda acepción: *"2. Der. Cometer alguno de los delitos que se caracterizan por el lucro como fin y el engaño o abuso de confianza como medio."*, nótese que, en realidad, tal definición está lejos de calzar con lo descrito en el tipo penal, toda vez que la estafa informática no requiere de un engaño ni tampoco el abuso de confianza como medio.

Es visible a todas luces que, el concepto estafa ha sido considerado al unísono por la doctrina como un delito en el que el sujeto activo perjudica en el patrimonio[87] a alguien mediante engaño o ardid, haciéndola incurrir en un error, provocando una lesión patrimonial para el sujeto pasivo o para un tercero, a pesar de ello y atendiendo nuestra legislación, nos encontramos con un desfase semántico importante, ya que se tituló el tipo penal 217 bis como una estafa[88], y

---

[87] Ver DONNA, Edgardo Alberto y DE LA FUENTE, Javier Esteban. *Aspectos generales del tipo penal de estafa*. En: Revista Latinoamericana de Derecho, año I, N° 1, 2004, p. 40: *"Asiste razón a Conde-Pumpido Ferreiro, cuando afirma que "los delitos contra el patrimonio en su conjunto son aquellos que atentan al patrimonio considerado como valor económico y que es perjudicado por la acción delictiva, estimándose como prototipo de ellos la estafa, que es el delito patrimonial por antonomasia, hasta el punto de llegar a afirmarse, no sin exageración, que el concepto de patrimonio nace por y para la estafa y se desarrolla a partir de sus exigencias" (Conde-Pumpido Ferreiro, Cándido, Estafas, Valencia, Tirant lo Blanch, 1997, p. 3)"*.

[88] Ver posición favorable a denominar el 217 bis del CP como estafa informática en: CHINCHILLA SANDÍ, Carlos. *Delitos informáticos: Elementos básicos para identificarlos y su aplicación*. Ediciones Farben, 1ª ed. San José, 2004, pp. 104-105: *"En realidad el nombre que se le brinda a cualquier figura penal, por parte del legislador, no es tan esencial, como sí su contenido. Esta labor de identificación con nombres a las normas penales es una técnica que se desarrolla con frecuencia en nuestro país, debido a una marcada influencia latinoamericana […] Por ello, no consideramos que el término "fraude informático" haya sido mal utilizado, pero sí preferimos uno más adecuado y claro, como la expresión "estafa informática", con la cual circunscribimos el campo de acción y regulación del delito específico del artículo 217 bis del Código Penal y, además, brindamos una mayor seguridad jurídica, puesto que "fraude informático" es un concepto muy amplio, donde se logran incluir conductas que no propiamente se trata de específicas "estafas informáticas".* Ver posición crítica a denominar el 217 bis del CP como estafa en: GUERRERO

no sólo eso, sino que se le consideró como una especie de estafa llamémosla "evolucionada" o "recargada", ya que atendiendo las circunstancias de nuestros tiempos, se le agregó el calificativo de ser "informática", todo ello, a pesar de que los elementos objetivos del tipo no describen una acción de esa naturaleza.

Y es que, aunque parezca un mero aspecto nominal e inofensivo, tratándose de derecho penal, sí resulta trascendente para todas aquellas personas procesadas por la comisión de dicha delincuencia. Si atendemos a la ansiada armonía del ordenamiento jurídico, al denominar el artículo 217 bis del CP como "estafa informática", se le está considerando como una verdadera "estafa" pero modernizada, e incluso más gravosa a criterio de quienes legislaron, fijándosele una pena de prisión desde esa perspectiva, lo cual, tal y como se verá termina siendo contraproducente en la dosificación penal. El profesor Castillo refiere: *"El artículo 217 bis del Código Penal tiene la función de llenar lagunas que se*

BARRANTES, Elízabeth y SALAZAR RODRÍGUEZ, Alonso. *Comentarios críticos a la reforma del CP que introduce la ley 9048 (sobre delitos informáticos en el derecho penal costarricense)*. En: Revista Judicial, N° 112, Costa Rica, 2014, p. 252: *"Es preciso antes señalar que técnicamente no es ninguna estafa, por ausencia de un sujeto pasivo que realice el acto dispositivo, sin embargo se asemeja a la hipótesis de la estafa triangular, la cual supone que el engañado y el estafado son personas diferentes. Sin embargo, en la estafa triangular el engañado tiene la facultad de realizar un acto dispositivo perjudicial para el estafado, de manera que el autor le produce a través de ese engaño, una lesión a su patrimonio y obtiene para sí o para un tercero un beneficio patrimonial antijurídico. En el caso de la aquí denominada "estafa electrónica" lo que el autor hace es "engañar" [utilizamos el término únicamente como una pseudodefinición estipulativa porque claramente no es un engaño, sino una manipulación] a la computadora (que sustituye al sujeto pasivo), y produce con esto que la computadora realice un acto dispositivo perjudicial para un tercero, desde luego, pues para la computadora no puede existir un perjuicio patrimonial en ningún supuesto."* Una de las razones (además de que el engaño o ardid no se encuentran descritos como elementos objetivos del tipo penal 217 bis del Código Penal) por la cual la estafa informática realmente no es una estafa, es porque hay una imposibilidad material y virtual, el computador o la máquina, simple y sencillamente no tiene la capacidad de ser inducida a error. Se debe hacer hincapié en que, es impreciso del todo hablar de engaño a una computadora; también deviene en impreciso el comentario respecto a indicar que *"no es un engaño, sino una manipulación"*, tal y como se verá, no siempre (según la redacción del tipo penal 217 bis del Código Penal) nos encontramos ante una manipulación del sistema informático. Nótese que todas estas confusiones e imprecisiones son derivadas por el hecho de haber denominado el numeral 217 bis del CP como una especie de estafa, entonces no es cierto, que denominándolo de esa manera, íbamos a obtener una mayor precisión y seguridad jurídica, tal y como lo refirió Chinchilla Sandí en el párrafo transcrito *supra* (quien por un lado indica que el nombre del tipo penal no es tan esencial, pero por otro lado dice que el nombre tiene la capacidad de dar mayor seguridad jurídica), en realidad sucede todo lo contrario, por lo tanto, el nombre otorgado a los delitos, es esencial, ya que debe existir una coherencia entre el título y el contenido, además ayuda a delimitar el tema y da una mejor comprensión no sólo a los operadores del derecho, sino al público en general, lo cual es más importante.

producen si se quiere aplicar el tipo penal de la estafa general a la manipulación de los datos o usos no autorizados a resultados patrimoniales de un sistema de procesamiento de datos (por medio de una computadora) […] Por ello, la interpretación del art. 217 bis Cód. pen. Debe orientarse por los criterios de interpretación del art. 216 Cód. Pen…"[89] Es decir, a pesar de ser tipos penales distintos en sus descripciones objetivas y subjetivas, se encuentran vinculados.

Ahora bien, continuando con el análisis del tipo penal, no se comparte la siguiente frase del penalista costarricense Ricardo Salas, quien, en referencia a la estafa informática, señaló: *"La diferencia con la estafa común empieza por el destino del engaño. En el artículo 216 se sanciona a "Quien induciendo a error a otra persona o manteniéndola en él…". **En la estafa informática no se induce a error a "alguien", sino a "algo"**, que consiste en la manipulación o influencia en el procesamiento o resultado de ese sistema automatizado de información, gracias al uso de datos falsos o incompletos, el uso indebido de estos o artificio tecnológico, incidiendo en el procesamiento de los datos o produciendo una información falsa, incompleta o fraudulenta. Nuevamente, además de cuál es el destino del "engaño", la diferencia básica con la figura común, es el modo en que se afecta el bien jurídico. En esta ocasión, el "engaño" que lleva a un daño se efectúa en un sistema como el descrito…"*[90] Afirmación similar realizó el abogado Carlos Chinchilla Sandí en el año 2004, al mencionar en su libro sobre delitos informáticos: *"Debemos partir de la distinción entre el **delito de estafa**- en su configuración genérica- (artículo 216 del Código Penal) y la **estafa informática** (artículo 217 bis del Código Penal*[91]*). En el primer caso, la estafa comprende el error en que se hacía incurrir a una persona, por medio del engaño, para conseguir un beneficio patrimonial ilegal para sí o para un tercero, logrando*

---

[89] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 66 y 67.

[90] SALAS PORRAS, Ricardo. *Derecho penal especial*. Editorial Investigaciones Jurídicas S.A, 1ª ed. San José, 2019, pp. 159 y 160. El resaltado no corresponde al original.

[91] Llama la atención que le denominara estafa informática al numeral 217 bis del CP, toda vez que para cuando escribió el libro Delitos Informáticos (2004), el tipo penal vigente se denominaba "fraude informático". El resaltado no corresponde al original.

lesionar el patrimonio ajeno. ***Esta descripción del delito objetivo muestra el problema del engaño dirigido en contra de una persona, pero no el engaño a una máquina o computadora, como el caso del cajero automático de los bancos. En el segundo caso el autor altera o manipula (engaño) el ingreso,*** *procesamiento y salida de datos de un sistema de cómputo, por medio de programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema, del cual se pueda generar un perjuicio para un tercero…"*[92]

Tales comentarios son desacertados en razón de que, al no ser la estafa informática un delito de auto lesión, consecuentemente se excluye la posibilidad de que exista un engaño dirigido hacia una máquina o un computador; con menos razón se puede considerar que, en la estafa informática se induce a error a "algo", toda vez que ese "algo" termina siendo una máquina, cuya función es procesar los datos que le son ingresados[93], un computador no puede hacerse una representación falsa de la realidad[94], circunstancia que descarta que pueda ser engañada. También, es una imprecisión conceptual igualar el verbo manipular a engañar, tales conceptos son distintos y no merecen ser confundidos.

El autor Sandro Abraldes, citado por Donna y De La Fuente, indicó al respecto: *"Debe, pues, desterrarse la inexacta apreciación de la realidad de las cosas que subyacen tras expresiones como 'engaño a una máquina', 'ordenador engañado que realiza un acto de disposición' y otras tantas semejantes. Porque, ni se engaña a la máquina – a lo sumo se engaña a alguien utilizando como*

---

[92] CHINCHILLA SANDÍ, Carlos. *Delitos informáticos: Elementos básicos para identificarlos y su aplicación*. Ediciones Farben, 1ª ed. San José, 2004, p. 44.

[93] Ver CEDANO OLVERA, Marco Alfredo, CEDANO RODRÍGUEZ, José Antonio, RUBIO GONZÁLEZ, José Antonio, y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010, p. 35: *"El lenguaje de máquina es el único que entiende la computadora, es su lenguaje por naturaleza. Sólo se pueden utilizar dos símbolos: el cero (0) y el uno (1). Es por ello que al lenguaje de máquina también se le llama lenguaje binario. La computadora sólo puede funcionar con bits; sin embargo, para el programador no resulta fácil escribir instrucciones tales como 10110011."*

[94] SÁNCHEZ DELGADO, Daniel. *La estafa. Análisis de sus elementos y problemática con los llamados delitos informáticos*. En: Revista Judicial. Tomo I. Año XX. N° 65, San José, 1997, p. 65.

instrumento la máquina– ni el ordenador realiza por error acto alguno de disposición – en todo caso, 'ejecuta' el traspaso patrimonial ordenado y dispuesto por quien ha efectuado la programación –" (Abraldes, Sandro F., La estafa mediante medios mecanizados, en L.L del 25 de junio de 1997)."[95]

De conformidad con lo anterior y para una mejor comprensión, se deben desechar los conceptos de engaño en el delito de estafa informática previsto en el numeral 217 bis del CP, no sólo porque no está contemplado dentro de los elementos objetivos del tipo, sino, además, porque conceptualmente hablando, es incorrecto referir que una máquina pueda ser engañada.

El mismo profesor Francisco Castillo realizó el siguiente comentario, cuya segunda parte creemos no es correcta: *"En la estafa general es necesario que la persona del engañado sea el mismo que hace el acto dispositivo.* ***Lo anterior no es posible en la estafa informática, en donde no siempre el engañado*** *y el que hace el acto dispositivo es el mismo."*[96] No queda claro por qué el autor analiza la presencia del engaño en la estafa informática, ya que, tal y como lo hemos referido, el engaño no es un elemento objetivo de ese tipo penal.

En los casos en que media un engaño como en la pesca de información, y posteriormente se hace un uso indebido de los datos de la víctima, podríamos sentirnos tentados a considerar la estafa general por mediar el engaño previo al uso indebido de datos, sin embargo, atendiendo el caso concreto, es aplicable la estafa informática en tanto, termina perdiendo interés la forma de obtención de la información por parte del sujeto activo, ya que lo que interesa para la subsunción de la conducta en el tipo penal 217 bis del CP, es que se influyó en el sistema de procesamiento de datos mediante el uso indebido de datos.

---

[95] DONNA, Edgardo Alberto y DE LA FUENTE, Javier Esteban. *Aspectos generales del tipo penal de estafa*. En: Revista Latinoamericana de Derecho, año I, N° 1, 2004, p. 68.

[96] CASTILLO GONZÁLEZ, Francisco. *La estafa informática de "Lege lata" y de "lege ferenda"*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 295. El resaltado no corresponde al original.

En razón de ello, es fundamental analizar cuáles sí son los verbos típicos introducidos por el legislador y la legisladora en el delito de estafa informática.

Verbos típicos de la estafa informática

Uso de datos falsos, incompletos, indebidos o de programación. Valerse de operación informática o artificio tecnológico

El artículo 217 bis del CP, describe que, el sujeto activo de la conducta debe incurrir en el verbo "usar", ya sea datos falsos, incompletos, indebidos, programación o valerse de una operación informática o artificio tecnológico o cualquier otra acción. Una vez realizado alguno de esos comportamientos humanos, necesariamente para subsumir la conducta en el tipo penal, debe influir o incidir en el procesamiento de los datos del sistema o dar como resultado información falsa, incompleta o fraudulenta, procurando obtener un beneficio patrimonial o indebido para sí o para otro. Es cierto que, el numeral en cuestión menciona los verbos "manipular" (el cual será analizado de manera independiente), "influir" e "incidir", siendo estos dos últimos producto de las acciones descritas *supra*.

La estafa informática es posible cometerla mediante los siguientes comportamientos humanos, tal y como lo señala el profesor Francisco Castillo en su obra: *"Dicho con todo el respeto para el colega Dr. Chinchilla, lo anterior, según nuestro criterio, es equivocado, pues las expresiones que definen las alternativas de acción son las siguientes: mediante el uso de datos falsos o incompletos, mediante el uso indebido de datos, de programación o bien mediante cualquiera otra acción que incida en el procesamiento de datos del sistema. De modo, entonces, que <u>influir</u> o <u>incidir</u> en el sistema automatizado de datos son resultados "intermedios" de las acciones punibles, que se dan antes de producir el resultado final, que es la transferencia de un valor económico del patrimonio del perjudicado al patrimonio del autor o de un tercero."*[97] Consideramos que lleva razón el señor

[97] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 80-81. El comentario fue realizado por el autor en razón de que Carlos Chinchilla Sandí había señalado en el libro "Derecho Penal Económico y Delitos Informáticos

Castillo, toda vez que “incidir” o “influir”, son situaciones que acontecen *a posteriori* de que el sujeto activo de la estafa informática usó datos falsos, incompletos o indebidos en el sistema de cómputo, o programó, valiéndose de alguna operación informática o artificio tecnológico.

En razón de que el tema en estudio está enfocado en la estafa informática mediante el uso indebido de datos, será necesario acercarnos al concepto, definiendo primero qué debemos entender por datos falsos o incompletos: *"...un dato es falso cuando contradice la realidad [...] Falsedad de los datos significa falsedad de la información codificada…"*[98] Por su parte, los datos incompletos son una subcategoría de los falsos, toda vez que terminan siendo datos no concordantes con la realidad. Ya sea mediante los datos falsos o incompletos, el sujeto activo debe influir en el resultado del equipo de procesamiento de datos.[99]

Ahora bien, cuando hablamos de uso indebido de datos o programación, nos referimos a datos que no son falsos ni incompletos, es decir, concuerdan con la realidad, razón por la cual *“se trata de una influencia no autorizada, por medio de datos o programación correctos, de personas no autorizadas o autorizadas para otros fines en el proceso automatizado de datos de una computadora.”* [100] De no contarse con esta modalidad delictiva, serían impunes algunas conductas, entre ellas: el sujeto activo que usa una tarjeta de crédito de la cual no es el titular,

---

(Ciberdelito)” (2013) lo siguiente, en referencia a la reforma del 2012 del artículo 217 bis Código Penal. *“De igual manera, este nuevo tipo penal incluye, además del verbo “influir” el nuevo supuesto de “manipular”, con lo que se logra una cobertura más completa a las posibles acciones a sancionar”*.

[98] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 87.

[99] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 88.

[100] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 95.

acción mediante la cual consigue dinero en efectivo gracias a que había obtenido la clave secreta.[101]

De tal manera, son bastantes los verbos incluidos en el tipo penal, sin embargo, lo esencial es que deben tener la capacidad de incidir o influir en el sistema, en razón de ello, deviene necesario darles contenido a los verbos infinitivos: manipular, influir e incidir:

Manipular

De conformidad con el DRAE, la palabra "manipular" se entiende como: *"1. Operar con las manos o con cualquier instrumento […] 3. Intervenir con medios hábiles y, a veces, arteros, en la política, en el mercado, en la información, etc., con distorsión de la verdad o la justicia, y al servicio de intereses particulares"*[102]. *Prima facie*, podemos referir que el verbo manipular tendría entonces una connotación en sentido amplio (acepción 1) y otra en sentido estricto (acepción 3). Por la materia y el contexto en el que nos encontramos, es necesario hacer un uso restrictivo del término, por ende, consideramos que lo correcto, según la redacción del tipo penal, será utilizarlo en su sentido estricto, el cual se amolda de mejor manera a la figura en estudio; por otro lado, el verbo en su sentido amplio es impreciso y laxo, no brinda seguridad jurídica.

El doctor Francisco Castillo señala que *"Manipular" es poner mano en algo o sobre alguien para controlarlo. Con relación a un sistema automatizado de procesamiento de datos, "manipular" significa cambiar o modificar el contenido de datos o programas almacenados o un ataque no permitido al sistema de procesamiento de datos en marcha para fines de enriquecimiento […] Cuando se ve la computadora como instalación, que requiere información de entrada ("input") sobre el programa (manipulación del programa) y que transforma los datos de*

---

[101] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 95.

[102] Consulta realizada el 05-08-2019, al ser las 16:47 horas. El subrayado no corresponde al original.

consola (manipulación de consola) en informaciones de salida ("output"), la manipulación del trabajo de una computadora puede ocurrir en cuatro fases. Esa manipulación puede afectar cualquiera de las modalidades de la acción punible, definida ésta como utilización de datos. Pero la manipulación de datos no cubre el uso no autorizado de datos y programas, conducta punible en el art. 217 bis Cód. Pen."[103]

Según dicho autor, en la manipulación de los datos de entrada *"...no se perjudica el funcionamiento del sistema de procesamiento de datos; es decir, los datos suministrados son trabajados ordinariamente, pues la computadora y el programa funcionan correctamente, solamente que con datos falsos..."*[104] Para una mejor comprensión, cabe plantearse entonces la siguiente pregunta: ¿Cuál es el motivo por el cual el doctor Francisco Castillo considera que el uso indebido de datos no corresponde al verbo "manipular"? Parafraseando al autor, él expone que cuando nos encontramos ante datos falsos introducidos al sistema, sí estamos ante un supuesto de manipulación, se puede entender que ello es porque la acción se realiza por medios hábiles con distorsión de la verdad (datos falsos), a diferencia de cuando se usan datos verdaderos pero de manera indebida, en cuyo caso, el sistema simplemente procesa la información y da un resultado, por lo tanto, en este último supuesto, sí se influye en el procesamiento de datos pero no se le manipula en sentido estricto.

¿Realmente un computador puede procesar información falsa? La respuesta es afirmativa, un programa informático cuenta con validaciones, siendo su tarea discernir si la información ingresada es cierta o es falsa, se asegura o certifica que los datos con que se alimenta el sistema sean coherentes. Cuando se tiene validación, se disminuye la posibilidad de trabajar con datos falsos, sin embargo, ello dependerá de cada caso en concreto; lo cierto es que, un sistema informático podría dar un error si no valida los datos suministrados. La validación

---

[103] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 73. El resaltado no corresponde al original.

[104] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 74.

de un sistema informático permite que la entrada de datos sea más fidedigna, más confiable, hay sistemas que no tienen validaciones toda vez que éstas requieren más trabajo de la persona encargada de la programación, *ergo*, es más fácil que le ingresen datos falsos.

En cuanto a la manipulación de datos (manipulación de la consola), el jurista nacional Francisco Castillo señala que se da cuando: *"...el autor, con la ayuda de una consola, manipula el manejo de un sistema de procesamiento de datos o de una computadora. En este caso se procesan datos correctos en un programa de computadora que funciona correctamente. Como consecuencia de ello, los datos que se trabajan correctamente son cambiados conforme la voluntad del autor"*[105].

Referente a la manipulación de programa, indica Castillo: *"El autor cambia el programa de computación cuando reescribe una parte del programa o borra una parte de éste, cuando instala un nuevo programa o cuando, con la ayuda de programas creados por él, cambia los programas almacenados con la finalidad de lograr un procesamiento de datos favorable y provechoso. El autor puede ejecutar la manipulación del programa sea modificando un programa existente e instalado o bien instalando un nuevo programa. Si el autor modifica un programa existente se trata de una inputmanipulación, porque adicionalmente al cambio de ese programa se produce el procesamiento no permitido de los datos existentes. Precisamente por este cambio es que el autor trabaja de manera no permitida los datos existentes […] Una diferencia entre manipulación de programas y manipulación de datos de salida solamente se puede establecer con relación al contenido de los datos almacenados y su diferente función, porque los programas dirigen los procesos en la Unidad Central y en esa función permanecen, mientras que otros datos son objeto de manipulaciones de datos de entrada o de datos de salida, de los procesos dirigidos por el programa.* ***Por consiguiente, el objeto y el medio de la manipulación de entrada y la manipulación de programas no se***

[105] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 75.

***diferencian significativamente**. Si el programa es desde el inicio constituido de manera incorrecta, esto ocurre porque desde el inicio se cambiaron los datos, porque se aportaron nuevos datos o porque se borraron los datos existentes. Lo mismo ocurre en los casos de cambio del programa o en los casos del efecto sobre un programa en marcha, casos que solamente son posibles por aportes de datos de entrada que cambien las órdenes en que consisten los programas."*[106]

Sostiene dicho autor que, la única forma de manipulación termina siendo aquella de los datos de entrada, que contempla la manipulación de programas y de consolas, en tanto requieren una manipulación inicial de datos, sin embargo, no se perjudica el funcionamiento del sistema de procesamiento de datos, es decir, tanto la computadora como el programa funcionan de manera adecuada, sólo que con datos falsos. A criterio de Castillo González, esa situación revela que *"las llamadas manipulaciones de entrada, de programas, de consola y de salida no sirven para describir la acción castigada en el delito de estafa informática. Incluso la manipulación de datos de entrada […] solamente se refiere a datos falsos o incompletos, siendo que nuestro legislador castiga en el art. 217 bis Cód. pen. no solamente el uso de datos falsos o incompletos, sino también el uso indebido (sin autorización del derecho-habiente) de datos o de programas."*[107]

El pensamiento del autor es que, en aquellos casos de manipulación en cualquiera de sus cuatro manifestaciones, lo que debe prevalecer es la figura de la estafa informática pero en su modalidad de uso indebido de datos, concreta su idea al indicar: *"Lo cierto es que ya en la reforma del 2001 y en la reforma por ley 9048 de 10 de julio del 2012 del art. 217 bis Cód. pen., la manipulación de datos de entrada, la manipulación de programas y la manipulación de datos de salida no es la única acción delictiva prevista en ese artículo. Por un lado, el legislador sanciona el uso indebido de datos o de programas, caso en el cual hay un empleo*

---

[106] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 76-78. El resaltado no corresponde al original.

[107] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 79 y 80.

sin permiso del titular de un dato o un programa, sin que haya una manipulación en sentido estricto. Por otro lado, el legislador, dice claramente que la conducta punible se realiza "por cualquier otra acción que incida en el procesamiento de datos o que dé como resultado información falsa, incompleta o fraudulenta". Las otras acciones punibles a las que se refiere el legislador en el art. 217 bis Cód. pen. son "mediante el uso indebido de datos, programación, valiéndose de alguna operación informática o tecnológica". Si fuera cierta la tesis que sustenta el Dr. Chinchilla y la Sala Tercera[108]*, de que la estafa informática se realiza cuando hay manipulación de datos de entrada, manipulación de programas y manipulación de datos de salida, dejaríamos por fuera el uso indebido de datos, interpretación que estaría en contra del texto claro y expreso del 217 bis Cód. pen.*"[109] Consideramos que dicho razonamiento es correcto, más si valoramos que independientemente de los datos que sean usados (falsos, incompletos o indebidos), el actuar humano en la estafa informática implicará siempre un uso indebido de datos y no siempre una manipulación en sentido estricto.

Una circunstancia que debe quedar claramente delimitada, es que cuando se habla de manipulación, debemos entender que se produce *"una alteración en el sistema de almacenamiento y tratamiento de datos. Esta alteración debe consistir en el funcionamiento anómalo del sistema, es decir, la acción de manipular debe incidir sobre el proceso mismo del funcionamiento del sistema provocando resultados inadecuados o extraños a los que debería arrojar. El uso indebido de datos personales del usuario, por ejemplo, el acceso autorizado al home banking de la víctima, pero la transferencia no autorizada de dinero electrónico a la cuenta*

---

[108] Ver resolución número 2006-00148 del 24 de febrero de 2006, de las 09:00 horas de la Sala Tercera de la Corte Suprema de Justicia: *"De acuerdo a la redacción de la norma en el CP vigente, la acción del sujeto activo consistirá en* ***influir*** *en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de* ***incidir*** *en el proceso de los datos del sistema. Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos a seguir, que si alguno se altera fraudulentamente, incidirá en el resto del proceso…"*

[109] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 83.

del autor o de un tercero, o el pago no autorizado de servicios personales no encuadran dentro de los presupuestos normativos de la materia de prohibición. Sin manipulación de sistemas o programas informáticos no existe este tipo de fraude."[110] Es cierto que, esa posición la expone el autor Gustavo Aboso desde el derecho penal argentino, sin embargo, considero que la misma es posible aplicarla en Costa Rica, toda vez que, cuando existe uso indebido de datos, no se está manipulando el sistema, en lo que se incurre es en un "influir", extremo contemplado en nuestro artículo 217 bis del CP, incluso desde que se denominaba "fraude informático".

Ciertamente no existe ningún criterio diferenciador en el artículo 217 bis del CP, mediante el cual se discrimine, si prevalece la manipulación en el ingreso de datos o el uso de datos indebidos, no obstante, ambas descripciones no deben confundirse, el uso de datos constituye el verbo del tipo penal, mientras tanto, la manipulación en sentido estricto es una consecuencia que debe cumplir el sujeto activo después de usar datos falsos o incompletos, según lo explicado párrafos atrás. Incluso podría afirmarse que el uso indebido de datos, ya contiene de por sí, una manipulación en sentido amplio.

A pesar de que consideramos que manipular no constituye el verbo rector del tipo penal, resulta importante delimitar dicho concepto, es así como, si recurrimos a una interpretación restrictiva, cuando se pretenda utilizar el verbo "manipular" para el uso de ingreso de datos, estos últimos deben estar caracterizados por ser falsos o incompletos (manipulación en sentido estricto). Si los datos usados sin autorización son verdaderos y/o completos, estaríamos ante un caso de manipulación en sentido amplio. Nótese que en ambos supuestos nos encontramos ante un uso de datos indebidos. Podría entonces afirmarse que, cuando se habla de "uso indebido de datos", no se contemplan únicamente aquellos datos verdaderos que son usados sin autorización del titular, sino también, aquellos supuestos en los cuales, el sujeto activo hace uso de datos

[110] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 319.

falsos o incompletos. Se hace hincapié en que, cuando exista un uso indebido de datos verdaderos en el sistema informático, no se está ante una manipulación estricta, toda vez que la información utilizada no es falsa.

El doctor en Derecho Penal y profesor de la Universidad de Valladolid, España, Antonio Mª Javato Martín, con un enfoque del derecho español, pero con similitudes a lo indicado por el profesor Castillo González, señala: *"El elemento determinante de la nueva modalidad defraudatoria […] es la existencia de una manipulación informática. Dado el carácter abierto e inconcreto de la fórmula empleada se han suscitado dos interpretaciones en la doctrina […] Una amplia, mayoritaria, tanto doctrinal y jurisprudencialmente, que destaca la consecuencia última de la alteración del resultado del procesamiento automatizado –el qué– y no tanto la forma de la acción realizada –el cómo–. De tal forma que por manipulación habría de entenderse cualquier alteración del resultado de un procesamiento electrónico de datos.* ***La otra, más restringida, que atiende no tanto a las consecuencias sino al objeto sobre el que se actúa, descartando la intervención sobre los datos y sobre el hardware e incluyendo únicamente las actuaciones manipulativas sobre las instrucciones de procesamiento automatizado del sistema informático (software)*** *[…] En este sentido, cabe distinguir entre: 1) Manipulación previa (en la fase de input); 2) Manipulación del programa; 3) Manipulaciones posteriores o en las salida de datos (output) […] En su ejecución práctica, la* ***manipulación de carácter previo puede ser tanto activa, en sentido estricto (modificando datos reales o añadiendo otros ficticios)*** *como omisiva (realizando la manipulación mediante un dejar hacer). Si bien es cierto que este grupo de supuestos no llegan a alterar la configuración de las instrucciones del programa,* ***por lo que en sentido estricto no habría manipulación informática****, sin embargo, como ya anteriormente se ha expuesto, el mantenimiento por la doctrina y los tribunales de la concepción amplia permite incluirlos en el perímetro de la acción típica […] Por su parte, en la manipulación del programa se modifican las instrucciones del programa alterando o eliminando alguno de los pasos o introduciendo partes nuevas en el mismo. (Así, por ejemplo,*

la "técnica del salami" –Salami technique–, o la del "Caballo de Troya –Troyan horse–)…"[111]

En cuanto al uso indebido de datos, consistente en que el sujeto activo hace uso de una tarjeta bancaria de su verdadero titular en un cajero automático retirando dinero, el autor Javato Martín, considera que la conducta sí se puede subsumir en el verbo "manipular", pero en el concepto ampliado.[112] En ese mismo sentido, el profesor Castillo, haciendo alusión a dicho derecho europeo, señala que, en lo referente a los datos introducidos (no falsos) en un sistema informático por el sujeto activo, provoca una intervención no autorizada, siendo que se dificulta subsumir la conducta en el artículo 248.2 del CP de España, ello sin ampliar el sentido del término "manipulación".[113] Llama la atención lo señalado por el profesor Castillo, toda vez que, la reforma del Código Español LO-2010 del 22 de junio de 2010, contempló la posibilidad de procesar a una persona por el delito de estafa cuando: *"c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero."* Es decir, no resulta cierto que se deba recurrir al verbo manipular, para sancionar un eventual uso indebido de datos, puesto que el caso de las tarjetas bancarias, ya había sido contemplado por el legislador español[114], tema que será profundizado en el acápite de derecho comparado.

---

[111] JAVATO MARTÍN, Antonio Mª. *Sobre: "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"*. En: Revista Electrónica de Ciencia Penal y Criminología. N° 10-r5, ISSN 1695-0194, Valladolid, 2008, pp 5 y 6. Versión electrónica en: http://criminet.ugr.es/recpc/10/recpc10-r5.pdf.

[112] JAVATO MARTÍN, Antonio Mª. *Sobre: "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"*. En: Revista Electrónica de Ciencia Penal y Criminología. N° 10-r5, ISSN 1695-0194, Valladolid, 2008, p. 8. Versión electrónica en: http://criminet.ugr.es/recpc/10/recpc10-r5.pdf.

[113] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 84.

[114] Ver SALINERO ALONSO, Carmen. *Delitos contra el patrimonio (III). Defraudaciones: Estafa. Apropiación indebida. Defraudaciones de fluido eléctrico y análogas. En: Lecciones de derecho penal: delitos contra la vida, las personas y el patrimonio, parte especial. Tomo III. Editorial Jurídica Continental, 2ª ed. San José, 2017, p. 512. "La LO 5/2010, de 22 de junio, introdujo una nueva modalidad de estafa que no solo vino a colmar lagunas de punibilidad, como es el caso del uso*

En cuanto al último tipo de manipulación, refiere Javato Martín: "*las manipulaciones efectuadas en la fase output generan directamente una alteración en el reflejo exterior del resultado del procesamiento automatizado de datos. Como tal manipulación en el resultado, la misma puede llevarse a cabo, bien en el reflejo último en el papel escrito mediante impresora, bien en el registro en la banda magnética cuando los datos van a ser transmitidos a otros ordenadores. En esta fase output, indica el autor, se situaría la frontera de lo que constituye una manipulación de datos punible conforme al delito que nos ocupa, de tal forma que no se podrán calificar de estafa electrónica las alteraciones producidas después de finalizado el proceso con la salida de los mismos…"*[115]

Por su parte, cuando se hace referencia a la manipulación de los datos de salida, el profesor Francisco Castillo, indica que en realidad no se trata *"de una manipulación de computadora"*[116], por lo general consiste en: *"una falsificación de datos correctamente elaborados por el sistema de procesamiento de datos o el impedimento de la impresión de datos correctos, elaborados por este sistema de procesamiento de datos."*[117]

Creemos que el siguiente comentario del profesor Francisco Castillo es correcto: *"El art. 217 Cód. pen. castiga a quien, en perjuicio de otro y con ánimo de enriquecimiento "…manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información…". La frase no es correcta, pues el verbo manipular sale sobrando, dado que* ***una manipulación***

---

ilegítimo de datos obrantes en tarjetas de crédito para realizar compras en internet, sino que también zanjó la discusión de algunos supuestos dudosos –el uso de tarjetas ajenas para extraer dinero de cajeros automáticos debía para algunos autores subsumirse en el robo con fuerza en las cosas—".

[115] JAVATO MARTÍN, Antonio Mª. *Sobre: "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"*. En: Revista Electrónica de Ciencia Penal y Criminología. N° 10-r5, ISSN 1695-0194, Valladolid, 2008, p. 6. Versión electrónica en: http://criminet.ugr.es/recpc/10/recpc10-r5.pdf.

[116] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 78.

[117] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 79.

solamente es punible en la medida en que influya en el resultado del trabajo del sistema automatizado de datos. Influencia en el procesamiento automatizado de los datos del sistema debe haber en todas las modalidades de acción descritas en el artículo 217 bis Cód. Pen*. (uso de datos o programas falsos o incompletos, el uso indebido de programas o de datos en el procesamiento automatizado de datos).”*[118]

Influir

El verbo infinitivo “influir”, tal y como lo refirió el profesor Castillo, es un resultado intermedio de la acción humana realizada por el sujeto activo, es definido por DRAE como: *“Dicho de una cosa: Producir sobre otra ciertos efectos; como el hierro sobre la aguja imantada, la luz sobre la vegetación, etc*...” La palabra efectos se debe entender como: *“**1.** m. Aquello que sigue por virtud de una causa. La fiebre es un efecto de la gripe […] **3.** m. Fin para que se hace algo. El efecto que se desea. Lo destinado al efecto…”*

Se desprende entonces que para que la conducta sea típica, debe producir efectos en el sistema informático, y ello lo alcanza el sujeto activo de la conducta mediante el uso de datos falsos, incompletos o indebidos, así como cualquier otra acción con dicha capacidad. Consideramos que causar efectos es poner en marcha el sistema para obtener un resultado.

El profesor Francisco Castillo considera atinadamente que: *“Para que la acción del autor influya en el sistema del procesamiento automático de datos, es necesario que el comportamiento del autor cocause el resultado del procesamiento automatizado de datos,* ***cocausación que ocurre cuando el resultado del procesador automático de datos no sería el mismo resultado al***

[118] CASTILLO GONZÁLEZ, Francisco. *La estafa informática de “Lege lata” y de “lege ferenda”*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 292. El resaltado no corresponde al original.

que llegó sin la acción del agente.”[119] Precisamente, si suprimimos hipotéticamente la acción del sujeto activo, el resultado no se hubiera provocado, razón por la cual sí existe una influencia en el sistema automatizado de datos.

Incidir

Nos encontramos ante otro resultado intermedio de la acción humana en el delito de estafa informática, que se presenta antes de que se produzca el resultado final, consistente en transferir el valor económico de la víctima hacia el patrimonio del imputado o de un tercero. Dicho concepto es entendido por el DRAE como: *“3. Repercutir (II causar efecto una cosa en otra)”*. Y este último como: *“Dicho de una cosa: Trascender, causar efecto en otra.”* Lo que ocurre con el verbo incidir en el tipo penal, es que con la acción humana se debe causar[120] efecto en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta.

El profesor Francisco Castillo, cuando se refiere a las “modalidades de la acción punible” del artículo 217 bis del CP, indica: *“Es esencial que el sistema automatizado de datos se encuentre en marcha (en funcionamiento). Esta característica de la estafa informática no ha sido puesta de manifiesto por la doctrina ni por la jurisprudencia nacionales, con excepción de algunas sentencias de la Sala Tercera de la Corte Suprema de Justicia”*[121] (el autor transcribe un extracto de una resolución de la Sala Tercera, sin embargo, no precisa el número de la misma, únicamente refiere que es de las 10:55 horas del 06-03-2009). Al respecto se debe indicar que Castillo González lleva razón puesto que, un sistema automatizado de datos que no se encuentre en funcionamiento o en marcha (se

[119] CASTILLO GONZÁLEZ, Francisco. *La estafa informática de “Lege lata” y de “lege ferenda”*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 293. El resaltado no corresponde al original.

[120] CASADO, Laura. *DICCIONARIO DE SINÓNIMOS JURÍDICOS*. Editorial Valleta, 2ª ed. Buenos Aires, 2004, p. 167: Señala que “causar” es sinónimo de “incidir”.

[121] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, 2016, p.85.

hace hincapié en que el autor iguala ambas frases), estaría imposibilitado para que se le ingresen datos, almacenarlos, procesarlos y emitir un resultado, es decir, estaría inerte. Ahora bien, no queda claro el motivo por el cual, el autor para respaldar su comentario, recurre al siguiente extracto de la resolución de la Sala Tercera, la cual, después de transcribir el antiguo 217 bis del CP, señala: *"En el presente caso, R. no manipuló los datos del sistema, ni influyó en su procesamiento, no hizo algo distinto a lo que hubiera hecho la ofendida con su tarjeta de débito, de manera que su conducta no encuentra en el tipo penal de examen. Este tema ha sido tratado en otras sentencias de esta Cámara; así, en un caso similar se explicó: 'De acuerdo a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en* ***influir*** *en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas* ***que han de incidir*** *en el proceso de los datos del sistema. Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de datos, es decir, en la realización de las instrucciones de un sistema. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos a seguir, que si alguno se altera fraudulentamente, incidirá en el resto del proceso. El usuario aparece al final de ese proceso, y en términos generales, no lo puede modificar. Para hacerlo, requiere el ingreso al sistema, y usualmente debe poseer ciertos conocimientos."*[122] Nótese que ese extracto, el cual Castillo asume como correcto, no hace referencia a la necesidad de que el sistema automatizado de datos tenga que estar en funcionamiento, pero en todo caso, el profesor Castillo al asumir esa posición, está diciendo que no se influyó en el procesamiento al utilizar los datos de la tarjeta de débito de la agraviada, puesto que la acción realizada por el sujeto activo fue exactamente la misma que hubiera realizado la ofendida, sin embargo, posteriormente en su libro, dicho autor señala con respecto a la "segunda modalidad de acción: uso indebido de datos o de la programación" (tesis que comparto): *"…Se trata de una influencia no autorizada, por medio de datos o*

[122] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, 2016, pp. 85 y 86. El resaltado y subrayado corresponden al original.

programas correctos, de personas no autorizadas o autorizadas para otros fines en el proceso automatizado de datos de una computadora…"[123]

Ahora bien, la circunstancia de si el sistema automatizado de datos está en marcha o en funcionamiento[124], consideramos es un asunto que debe definirse casuísticamente, por ejemplo, en el caso del sujeto activo que hace uso indebido de la tarjeta y de la clave de acceso del titular en un cajero automático, por medio del cual retira dinero, podríamos plantearnos las siguientes interrogantes: ¿Estaba en funcionamiento o en marcha el cajero automático con el solo hecho de estar encendido (previo a que se le introduzca la tarjeta o clave de acceso? O ¿Hasta tanto un usuario no haga uso del cajero automático, implica que dicha máquina no estaba en funcionamiento y es más bien la introducción de la tarjeta la que pone en marcha el sistema?

Nuestro parecer es que, el cajero automático se encuentra en funcionamiento desde el momento es que está encendido, recibiendo energía y tiene la capacidad de aceptar una tarjeta y de dispensar el dinero, es decir, no se encuentra inactivo, *ergo*, cuando el sujeto activo introduce la tarjeta y la clave, si bien, no está poniendo en funcionamiento el sistema automatizado, lo cierto es que, sí está influyendo en el sistema, pero en el flujo de ejecución de la etapa de autenticación. Sin embargo, aunque no adoptemos esa interpretación, y nos inclinemos por la segunda posición, diciendo que el cajero automático estaba "dormido" o inactivo, y entró en funcionamiento o en marcha desde el momento en que el sujeto activo le introdujo indebidamente la tarjeta e ingresó la clave de acceso del titular, no significa que estemos descartando la influencia en el sistema en el proceso de autenticación de la persona usuaria, es decir, en ambos supuestos, podemos afirmar que, sí se está influyendo en el sistema automatizado

[123] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 95.

[124] Ver CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 114 y 115: *"La doctrina dominante considera que quien pone en funcionamiento el sistema de procesamiento de datos tiene influencia sobre éste. Lo cierto es que no hay diferencia en el hecho de que el funcionamiento del sistema de procesamiento de datos esté ya en funcionamiento o sea echado a andar por la acción del delincuente."* (subrayado del original).

de datos, en una etapa de autenticación de la persona usuaria y demás procesos para obedecer los comandos, dispensar el dinero o realizar cualquier otra transacción en daño del patrimonio del titular de la cuenta. En conclusión, podemos afirmar que, es relativo el momento en que, se pone en marcha o en funcionamiento un sistema informático, ello dependerá de cada caso en concreto.

De la redacción literal del numeral 217 bis del CP, debemos plantearnos los siguientes cuestionamientos: ¿Para influir en un procesamiento de datos es necesario que el programa esté en funcionamiento o en marcha? O ¿Es posible influir en un procesamiento de datos sin que el programa esté en funcionamiento o marcha? Considero que como una situación elemental, estaríamos ante un delito imposible si se intentara influir en un sistema automatizado de datos que no esté en funcionamiento, ya que el mismo no es capaz de procesar la información o los comandos que se le intenten ingresar, es decir, aunque el numeral 217 bis del CP no establezca dentro de sus elementos objetivos que el sistema informático debe estar en funcionamiento, se debe entender como requisito indispensable esa situación, puesto que de lo contrario, dicho numeral carecería de toda lógica.

Dosificación penal de la estafa informática en comparación con la estafa convencional

Se ha venido indicando que la estafa informática describe comportamientos humanos que realmente no son estafadores, sin embargo, el legislador y la legisladora, en lo que podríamos denominar una técnica legislativa incorrecta, decidieron bautizarlo de esa manera. Según el profesor Castillo, *"Tanto los datos falsos como los datos incompletos se orientan al concepto de hechos falsos de la estafa general"*[125]; quizá ese es un elemento indicador de por qué se le tituló de esa manera sin serlo. Sin embargo, las discusiones legislativas al respecto serán analizadas en otro capítulo. Por el momento conviene visibilizar un elemento trascendental, relacionado con la pena prevista en abstracto por quienes legislan, para el numeral 217 bis del CP, ello en comparación con la estafa general del

[125] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 88.

numeral 216 del mismo cuerpo normativo, en ese sentido se realiza el siguiente cuadro comparativo entre la estafa general y la estafa informática:

Tabla 3. Dosimetría penal entre estafa general y estafa informática

Gradiente de penas	**Estafa general** **(artículo 216 Código Penal)**	**Estafa informática (artículo 217 bis Código Penal)**
Pena base	De 2 meses a 3 años de prisión (monto defraudado no exceda diez veces el salario base)	De 3 a 6 años de prisión
Pena agravada	De 6 meses a 10 años de prisión (monto defraudado exceda diez veces el salario base)	De 5 a 10 años de prisión (“si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.”)
Aumento de la pena *“...cuando los hechos señalados los realice quien sea apoderado o administrador de una empresa que obtenga, total o parcialmente, sus recursos del ahorro del público, o por quien, personalmente o por medio de una entidad inscrita o no inscrita, de cualquier naturaleza, haya*	Pena base y agravada pueden ser aumentadas en un tercio: Pena base: De 2 meses y 20 días a 4 años de prisión Pena agravada: De 8 meses a 13 años y 3 meses de prisión	NO

obtenido sus recursos total o parcialmente del ahorro público".		

Si se comparan los rangos de penas previstos en abstracto, se determina lo siguiente: La estafa informática en su forma de comisión simple prevé una pena mínima de 3 años de prisión, y de 5 años en su modalidad agravada, extremos que están muy por encima de los mínimos de prisión previstos en abstracto en la estafa general: 2 meses (pena base), 2 meses y 20 días (pena base aumentada en un tercio), 6 meses (pena agravada) y 8 meses (pena agravada aumentada en un tercio). Se evidencia entonces, una desproporción importante, a pesar que ambos tipos penales tutelan en principio el mismo bien jurídico, sin embargo, las consecuencias procesales para quien deba descontar esas penas serán muy distintas, aun cuando se impongan los extremos mínimos, por ejemplo: la imposibilidad de optar por salidas alternas como la suspensión del procedimiento a prueba y la conciliación[126], ante la modalidad agravada de la estafa informática, tampoco permite conceder el beneficio de ejecución condicional de la pena, previsto en el artículo 59 y siguientes del CP[127]. Y es que, si se analiza que una de las causas por las cuales se agrava el delito de estafa informática, se presenta cuando la conducta es cometida en contra de *sistemas de información públicos, sistemas de información bancarios y de entidades financieras*, podríamos inferir *prima facie,* que esa es la modalidad de comisión más frecuente, convirtiendo la agravante en regla y no en excepción, ya que si bien, para llegar a una conclusión certera se hace necesario realizar un estudio estadístico, que escapa a los alcances de esta investigación, al menos, de la revisión jurisprudencial efectuada, se puede adelantar que la mayoría de casos conocidos en fase de impugnación,

[126] Institutos procesales establecidos en los artículos 25 y 36 del CPP, respectivamente, los cuales exigen como una condición *sine qua non*, la procedencia de la suspensión condicional de la pena.

[127] CP. Art. 59: *"Condena de ejecución condicional. Al dictar sentencia, el Juez tendrá la facultar de aplicar la condena de ejecución condicional cuando la pena no exceda de tres años y consista en prisión y extrañamiento."*

por no decir todos, están ligados a esa modalidad de comisión agravante como se verá.

Vale mencionar que la sola previsión en abstracto de un extremo menor de 3 años de prisión, en la modalidad simple del delito de estafa informática, pone en riesgo la posibilidad de optar por el beneficio de ejecución condicional de la pena, por cuanto el mínimo aumento que pueda ser aplicado por el Tribunal de sentencia, por ejemplo, un día, cercena definitivamente la aplicación de ese instituto. Diferente situación acontece ante el delito de estafa general, ya que aun y cuando, el Tribunal sentenciador eleve las penas mínimas, por ejemplo, en otro tanto, ni siquiera se acerca al límite establecido como requisito para la precedencia del beneficio mencionado. Es decir, el margen de actuación que tiene la persona juzgadora en la dosificación de la pena, es mayor en el delito de estafa general, sin afectar la posibilidad de otorgar el beneficio, en resguardo de los principios *pro homine* y *pro libertate*.

Ahora bien, en la etapa de ejecución de la pena, la elevación de los mínimos establecidos en abstracto, y sin incluir los eventuales aumentos en la imposición de la pena, inciden en el tiempo que deberá esperar la persona condenada, para optar por los distintos beneficios carcelarios, ya sea a nivel administrativo como judicial, así como en lo que respecta al plazo que durará inscrita la sentencia en el Registro Judicial[128].

---

[128] Artículo 11 de la Ley del Registro y Archivos Judiciales, N° 6723 y su reforma N° 9361 del 16 de junio del 2016: *"El Registro Judicial cancelará los asientos de las personas sentenciadas luego del cumplimiento de la pena, atendiendo los siguientes parámetros:*
a) Inmediatamente después de cumplida la condena impuesta, cuando la pena sea inferior a tres años o por delitos culposos.
b) Un año después de cumplida la condena impuesta, cuando la pena sea entre tres y cinco años.
c) Tres años después de cumplida la condena impuesta, cuando la pena sea entre cinco y diez años.
d) Cinco años después de cumplida la condena impuesta, cuando la pena sea de diez años en adelante.
e) Diez años después de cumplida la condena impuesta, cuando la pena sea por delitos tramitados bajo el procedimiento especial de crimen organizado, según el artículo 2 de la Ley N.° 8754, Ley contra la Delincuencia Organizada, terrorismo, delitos sexuales contra menores de edad, homicidio calificado, feminicidio y delitos contra los deberes de la función pública.
f) En los casos de delitos cometidos por una persona en condición de vulnerabilidad y con familiares dependientes, el juez o la jueza de ejecución de la pena valorará la cancelación de los

No se omite mencionar que, en cuanto al extremo mayor de pena previsto en abstracto, la situación se invierte, toda vez que, la estafa general prevé una pena máxima de 13 años y 3 meses de prisión, según lo establecido en el último párrafo del artículo 216 CP, mientras tanto, la estafa informática prevé como extremo mayor 10 años de prisión en su forma de comisión agravada. De acuerdo con lo anterior, si bien, la estafa informática en cuanto al extremo mayor prevé una penalidad inferior, lo cual aparenta ser un aspecto positivo, lo cierto es que, el límite de la pena mínima en abstracto para el delito informático es más perjudicial, ya que ese extremo menor es el obligado a imponer por quienes juzgan, es decir, de allí se parte para definir el *quantum* de la pena y no a la inversa, por lo que el hecho de que el extremo mínimo de un tipo penal disponga una penalidad menos severa, en definitiva beneficia el principio de intervención mínima del Estado en la persona procesada, en tanto reduce el plazo por el cual verá privada su libertad.

En cuanto a las agravantes de la pena, se desprende que, en la estafa informática a diferencia de la estafa general, no se toma en cuenta el valor de lo sustraído para mayor punibilidad, pero sí se pondera en ambos tipos penales especiales impropios, una agravante para cuando el autor cumpla con determinadas funciones dentro de una empresa, tal y como se observa a continuación:

Tabla 4. Agravantes de pena en estafa general y estafa informática

Estafa general (artículo 216 CP)	**Estafa informática (artículo 217 bis CP)**
Sujeto activo: Una persona que ostente el cargo de apoderado o administrador de una empresa que obtenga, total o parcialmente, sus	**Sujeto activo:** Una persona que sea empleada con funciones específicas de administrar o dar soporte al sistema o red

asientos una vez cumplida la pena impuesta, con excepción de los delitos tramitados o bajo la tramitación del procedimiento especial de crimen organizado, según los términos de la Ley contrala Delincuencia Organizada, terrorismo, delitos sexuales contra menores de edad, homicidio calificado, feminicidio y delitos contra los deberes de la función pública.
Si la solicitud de certificación de juzgamientos se hace para fines laborales, de conformidad con los incisos e) y ñ) del artículo 13 de esta ley, el Registro Judicial de Delincuentes del Poder Judicial únicamente consignará en dicha certificación las existencias de los juzgamientos referidos en el inciso e) del presente artículo." (el resaltado no corresponde al original).

recursos del ahorro del público, o por quien, personalmente o por medio de una entidad inscrita o no inscrita, de cualquier naturaleza, haya obtenido sus recursos total o parcialmente del ahorro público.	informática o telemática O una persona que sea empleada, y que por las funciones que desempeña, tiene acceso al sistema o red informática o telemática, o a los contenedores electrónicos, ópticos o magnéticos

El profesor Francisco Castillo González, considera que la estafa informática se encuentra en una relación de exclusividad con respecto a la estafa general, además, tiene el papel de ser subsidiaria de la estafa común, siendo un tipo penal creado para capturar los casos que no se pueden subsumir en el artículo 216 del CP, por lo tanto, la estafa general excluye a la estafa informática en aquellas situaciones fácticas que puedan subsumirse en ambos tipos penales.[129] Agrega que para poder encuadrar la conducta en uno y otro tipo penal, es necesario determinar si la disminución patrimonial es consecuencia inmediata de una actuación errónea de una persona (estafa general); o si por el contrario, dicha disminución patrimonial es producto inmediato del funcionamiento de un sistema de procesamiento de datos (estafa informática).[130]

De conformidad con lo anterior, al confrontar el delito previsto en el artículo 217 bis del CP con su homónimo 216, logramos derivar que quienes legislaron, consideraron más reprochable, por lo menos en cuanto a su extremo mínimo de punibilidad, aquella conducta del agente consistente en el uso de datos indebidos, falsos o incompletos en un sistema automatizado; que aquella en la cual el sujeto activo induce a error a otra persona mediante engaño o ardid, ello a pesar de que ambas figuras protegen el bien jurídico patrimonio, y que la estafa general, tiene secuelas más severas en la persona física que se convierte en víctima, no sólo desde un punto de vista de su patrimonio, sino más importante, desde aspectos

[129] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 134 y 135.

[130] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 135.

emocionales. Tal reflejo legislativo consideramos que no es razonable, ello en virtud de que, la interrelación entre personas físicas es más íntima, que el hecho de usar una computadora o una máquina e insertar datos causando un perjuicio patrimonial, ya que la primera tiende a afectar directamente la psiquis de una persona víctima que confió en otra, precisamente debido a ese contacto directo con su victimario, el cual, en muchas ocasiones, según la experiencia y psicología, termina generando culpa en la víctima, además de la lesión en el patrimonio.

Ha existido una tendencia mundial a sustituir a las personas por las máquinas en diferentes campos[131], sin embargo, resulta ilógico e inhumano, sobreponer un computador a un ser humano, es decir, el hecho de considerar que engañar a otra persona sea menos reprochable que insertar datos indebidos en un sistema informático es algo inconcebible para el derecho penal actual, puesto que el derecho penal parte de una concepción personal, es decir, es para los seres humanos.

Con lo anterior, no pretendo promover una elevación de las penas mínimas del 216 del CP, sino que, las del 217 bis del mismo cuerpo normativo, deberían como mínimo ser equiparadas, ya que tal y como se encuentran estipuladas en la actualidad, devienen en incoherentes entre sí, atendiendo la armonía normativa que debe imperar en el ordenamiento jurídico. Véase que de todos los delitos informáticos vigentes en nuestro ordenamiento jurídico[132], la "estafa informática"

---

[131] Ver FROSINI, Vittorio. *Cibernética, Derecho, Internet y Sociedad*. Ediciones Olejnik, Santiago-Chile, 1ª ed. 2019, p. 70: *"Se trata precisamente de una evaluación de la ideología cibernética, en cuanto «la presencia de lo artificial en la vida de hoy representa un hecho cualitativamente nuevo […]. La extraordinaria proliferación de lo artificial tiende a hacer que el hombre se convierta en un agente de segundo grado, que anima y dirige máquinas que actúan directamente; el vivir en un mundo de artefactos influye de manera efectiva en la psicología del hombre; el artefacto de hoy no es solamente el producto de un proceso de modificación de la forma de lo natural, sino de una modificación de su substancia […]. La naturaleza se aleja cada vez más del hombre, que parece reconocerse e identificarse con su proyecto creativo»."*

[132] En Costa Rica se introdujeron los delitos informáticos mediante las siguientes leyes: **1)** Ley N° 8184 del 24 de octubre de 2001 que crea el fraude informático en el artículo 217 bis del Código Penal; **2)** Ley N.º 9048 del 10 de julio de 2012, titulada: *"Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal"*, publicada en el Alcance N.º 172 de La Gaceta N.º 214 del 06 de noviembre de 2012; y **3)** Ley N° 9135 del 24 de abril de 2013, titulada*: "Reforma de los artículos 196, 196 bis, 230, 293 y 295 y*

es uno de los que tiene mayor penalidad prevista en abstracto, circunstancia que refleja el interés de la sociedad actual, en "proteger" mediante leyes, de manera más estricta el patrimonio[133], que otros derechos de las personas, como la intimidad, privacidad e incluso la autodeterminación informativa[134].

Otro elemento que llama la atención es que, el delito de estafa general es un delito de resultado, mientras tanto el de estafa informática incorpora dos posibilidades, sanciona al sujeto activo que "procure" u "obtenga", es decir, se trata de una mixtura, convirtiéndose en una construcción legislativa sui géneris, ya que es de resultado y de peligro, ante ese panorama, en acatamiento a los lineamientos de un sistema penal garantista, consideramos que la estafa informática prevista en el numeral 217 bis del CP, debería entenderse como un delito de resultado, de manera que posibilite la existencia de la tentativa; y no la

---

adición del artículo 167 bis al Código Penal", publicada en el Alcance N° 78, de La Gaceta N° 80, del 26-04-2013.

[133] Ver FERNÁNDEZ MORA, Christian. *La racionalidad tecnológica de la justicia penal en Costa Rica y su (Des) Humanización*. En: Revista Digital de la Maestría en Ciencias Penales de Universidad de Costa Rica. Homenaje al Prof. Dr. Francisco Castillo González en sus 70 años. N° 5, ISSN: 1659-4479, 2014, pp. 126 y 127: *"Se trata, más bien, de una clara fachada de lo humano que es la justicia –no en su sentido ideal, sino en el sentido real o material- cuando pretende llevar hasta sus límites máximos la idea de la modernidad, de una racionalidad marcada por las reglas del mercado, donde las prácticas más democráticas se vuelven formas de sometimiento. Por eso Foucault señala que las democracias actuales, nos permiten vivir "…bajo un régimen de dictadura de clase, de un poder de clase que se impone a través de la violencia, incluso cuando los instrumentos de esta violencia son institucionales y constitucionales"*.

[134] LEANDRO CARRANZA, Hans Roberto. *Delitos de peligro abstracto: nuevos desafíos para la teoría del delito*. 1ª ed. San José. Editorial Investigaciones Jurídicas S.A., 2011, p.p. 70 y 71.: *"Por otro lado, no hay duda de que la sociedad moderna ha generado la necesidad de regular una serie de aspectos que anteriormente no estaban normados. Por ejemplo, el campo tecnológico y específicamente informático puede ser un instrumento idóneo para generar múltiples actividades repudiables como conocer las claves de las tarjetas de débito y, con ellas, realizar una cantidad indeterminada de transacciones que afectan el patrimonio de las personas, el ingresar a sistemas de seguridad y conocerlos, etc. Similar ocurre en materia de seguridad pública y seguridad ciudadana, aspectos que exigen una intervención del Estado pues todo ello genera un sentimiento de inseguridad que exige la regulación. Sin embargo, no es a través del abandono de principios básicos del Estado moderno como se puede lograr. No basta la simple creación de una norma y la creación arbitraria de un bien jurídico para estimar que el Estado ha evolucionado. El Estado Social implica más que eso, se deben buscar y construir mecanismos que nos permitan disfrutar de tales avances con seguridad, entendiéndose tal término en el más amplio sentido, es decir, como sinónimo de seguridad humana. Por ello, lo deseable es que la actividad desplegada por el Estado brinde una solución integral y no recurra a una normativización prohibitiva que implica una agresión importante como la que ofrece el Derecho Penal."*

consumación por solo el hecho de poner en peligro el bien jurídico, más atendiendo las vastas críticas acertadas que se hacen a los delitos de peligro[135], debido a que incurren en un adelantamiento de la barrera de punición. En ese sentido, el autor Leandro Carranza señala: *"Evidentemente, en el delito de lesión, el peligro ya se encuentra incluido en la misma norma; en otras palabras, en los delitos de lesión no se adelanta la sanción sino que el Derecho Penal responde como debería: como una reacción ante una acción que produjo un resultado prohibido. Se sanciona algo más que la simple desobediencia a una norma (…) No hay duda de que al exigirse la constatación de la lesión del bien jurídico se garantiza una disminución del ejercicio del ius puniendi, máxime que el Derecho Penal impone graves consecuencias a los ciudadanos que ejecutan dichas acciones que son "ataques institucionalizados" a derechos fundamentales (Ropero Carrasco, 2006: pág. 129)."*[136]

Pero no sólo nos encontramos ante un tipo penal que ostenta la condición de ser de resultado y de peligro, sino que además, es un tipo penal ambivalente, puesto que atendiendo las clasificaciones de los denominados delitos de peligro, termina siendo tanto de peligro concreto como de peligro abstracto, ya sea para el bien jurídico patrimonio o para cualquier otro bien jurídico tutelado[137], el mismo se

---

[135] Ver LEANDRO CARRANZA, Hans Roberto. *Delitos de peligro abstracto: nuevos desafíos para la teoría del delito*. 1ª ed. San José. Editorial Investigaciones Jurídicas S.A., 2011, p.p. 97 y 98: *"En Costa Rica, Castillo González, quien acepta la constitucionalidad de los delitos de peligro abstracto solamente cuando hagan referencia directa o indirecta a un bien jurídico, en uno de su más recientes libros (2009: págs. 49-79), sostiene que el artículo 28 de la Constitución Política nacional permite incorporar, dentro del ius puniendi, hechos que dañen el orden público y la moral siempre y cuando aquellos estén referidos directa o indirectamente a la protección de un bien jurídico individual. No comparto la posición de dicho autor. El artículo 28 de la Constitución lo que contiene es el principio de libertad personal. Interpretar que el orden público y la moral constituyen parte del ius puniendi implicaría una reducción al absurdo de esa libertad personal pues, por dicha vía, todo podría ser sancionado. No hay duda de que el orden público y la moral constituyen parte importante de las bases de una sociedad, sin embargo, pretender que el Derecho Penal asuma una función que comprendería no solo la totalidad del ordenamiento jurídico sino otros aspectos lejanos a lo jurídico sería pretender extender los brazos represivos del Estado de una manera peligros en un Estado de Derecho."*

[136] LEANDRO CARRANZA, Hans Roberto. *Delitos de peligro abstracto: nuevos desafíos para la teoría del delito*. 1ª ed. San José. Editorial Investigaciones Jurídicas S.A., 2011, p.p. 88 y 89.

[137] Ver LEANDRO CARRANZA, Hans Roberto. *Delitos de peligro abstracto: nuevos desafíos para la teoría del delito*. 1ª ed. San José. Editorial Investigaciones Jurídicas S.A., 2011, p.p. 102 y 103:

lee de la siguiente manera: *"...**con la cual procure u obtenga un beneficio patrimonial o indebido**…"*[138], lo cual denota una redacción confusa por parte de las personas legisladoras. Si bien se especifica que un bien jurídico es el patrimonio, lo cierto es que, la conducta del sujeto activo puede ser procurar ese beneficio patrimonial (delito de peligro concreto) u obtener dicho beneficio (delito de resultado). Y en cuanto a la frase *"un beneficio indebido"*, nos encontramos ante un tipo penal abierto, que no delimita cuáles son esos otros bienes jurídicos tutelados (delito de peligro abstracto).

Por esas razones y siendo que nos encontramos ante un tipo penal construido como si se tratara de un "Frankenstein" legislativo, la mejor interpretación que de él se puede hacer, respetando principios constitucionales, así como seguridad jurídica, es considerarlo como un delito de resultado, puesto que contiene la frase: *"obtenga un beneficio patrimonial"*.

Bien jurídico tutelado de la estafa informática

Para una menor comprensión del tema, nos referiremos en primera instancia al bien jurídico tutelado por la estafa general[139], el cual es: *"…un delito*

---

*"**Delitos de peligro abstracto-concreto**. En este tipo de delitos, se combinan elementos de los delitos de peligro abstracto con los de peligro concreto (Mendoza Buergo, 2001b y Rodríguez Montañes, 2004). En ellos, la peligrosidad no se deriva directamente de la ley, sino que la conducta deber ser analizada en forma objetiva por el juez y determinarse si era apta para lesionar el bien jurídico. En otras palabras, tendríamos una descripción típica de una conducta que realiza un delito de peligro abstracto. Sin embargo, con la sola acción no se tiene por realizado el tipo penal (que es lo propio de los delitos de peligro abstracto) sino que requiere de, al menos, una aproximación peligrosa al bien jurídico (lo que es propio de los delitos de peligro concreto), lo que hace necesario un juicio de valoración para determinar si esa acción produjo un peligro. Resulta cuestionable la existencia de este tipo de delitos: si el delito es de peligro abstracto con la sola realización de la conducta se realizaría el tipo y, si requiere de una puesta en peligro del bien, ya no estaríamos en presencia de un delito de peligro abstracto sino de uno de peligro concreto. Si añadimos que la acción realizada no encuadra en forma clara en el tipo penal y se requiere de un juicio posterior por parte de quien juzga para determinar si con ella se puso en peligro el bien jurídico, estaríamos generando una inseguridad adicional, pues se desconocería la extensión de la aplicación que se le daría a tales delitos, con lo que se violenta aún más el principio de legalidad…"*

[138] El resaltado no corresponde al original.

[139] Ver GARCÍA FIGUEROA, Alfonso; GASCÓN ABELLÁN, Marina; MARCILLA CÓRDOBA, Gema; PRIETO SANCHÍS, LUIS. *Argumentación jurídica*. Tirant lo Blanch. Valencia. 2014, p. 203: *"La razón última reside en una propiedad esencial de los ordenamientos jurídicos: su naturaleza unitaria y sistemática. Que el Derecho es sistemático significa que la interpretación de las*

de daño patrimonial causado a otro mediante engaño con la finalidad de obtener un beneficio patrimonial antijurídico. Según la doctrina y la jurisprudencia nacionales, se parte del concepto jurídico-económico del patrimonio, que es la totalidad de los bienes económicos de una persona, cuyo poder de disposición está jurídicamente aprobado y protegido…"[140]

Ahora bien, al hacer una comparación entre los tipos penales 216 y 217 bis del CP, refiere el doctor Francisco Castillo: *"…Diferencias entre el texto general de la estafa y la estafa informática existen solamente en tanto que la primera norma tiene elementos referidos a las personas, que son sustituidos en la estafa informática por el criterio de haber influido en el resultado del procesamiento de datos, con la cual el agente obtiene, en perjuicio de otro,* ***un beneficio patrimonial indebido para sí o para otro****…"*[141] En realidad, el artículo 217 bis del CP lo que dice es *"un beneficio patrimonial o indebido para sí o para otro*". Esa observación es esencial, puesto que, precisamente la redacción del artículo, atendiendo el principio de legalidad, permite que se puedan contemplar otros bienes jurídicos distintos al patrimonio. Indiscutiblemente, el hecho de suprimir esa letra "o" disyuntiva, provoca por un lado que, se parta de una premisa falsa, y por el otro, se entienda el patrimonio como único bien jurídico tutelado por el 217 bis del CP. El profesor Castillo no indica la razón por la cual suprime dicha letra, por ejemplo, si es que obedece a un tipo de interpretación funcional de la norma[142] o alguna otra razón.

---

disposiciones jurídicas no puede hacerse con absoluta independencia del resto de preceptos del ordenamiento. Ninguna norma es una isla."

[140] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 66.

[141] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 67. El resaltado no corresponde al original.

[142] Ver en ese sentido, GARCÍA FIGUEROA, Alfonso; GASCÓN ABELLÁN, Marina; MARCILLA CÓRDOBA, Gema; PRIETO SANCHÍS, LUIS. *Argumentación jurídica*. Tirant lo Blanch. Valencia. 2014, p. 260: *"Interpretación funcional (o lógica, o psicológica, o teleológica): consiste en atribuir significado a una disposición dejando de lado su significado literal y apelando, por el contrario, a la voluntad o la intención del legislador, o a los fines de la ley, es decir, a la ratio legis."*

El profesor Francisco Castillo, partiendo de que el articulado dice: *"beneficio patrimonial indebido"*, y no *"beneficio patrimonial o indebido"*, señala, por un lado: *"…**Como en la estafa general, en la estafa informática el bien jurídico tutelado es el patrimonio** y no el interés general de la capacidad de función del sistema computacional en la economía o en la administración pública. El bien jurídico tutelado por la estafa informática es únicamente el patrimonio y **es idéntico al bien jurídico tutelado por la estafa general**…"*[143] Pero al mismo tiempo, el autor sí admite la existencia de diferencias entre uno y el otro: *"…La estafa informática es un delito patrimonial especial, pues **el bien jurídico sería el patrimonio en su expresión especializada de datos y programas** […] Para nosotros, la estafa informática **protege el patrimonio en su dimensión de funcionamiento de sistemas automatizado de datos, de informaciones y de programas**…"*[144] Esta última referencia del autor, a mi criterio, permite contemplar que el 217 bis del CP, tutela otros bienes jurídicos, distintos al patrimonio. De esa manera, parece entenderlo el autor Roberto Lemaître, cuando señala que esa posición de Castillo, se aproxima al bien jurídico de la integridad de los datos en un sistema, como bien jurídico tutelado por la estafa informática, ello desde una perspectiva moderna[145]; en lo que no concuerdo con Lemaître, es que, ese sea el único bien jurídico tutelado por el 217 bis del CP, puesto que, como de manera acertada y al mismo tiempo él lo señaló en su obra: *"En primera instancia, el bien jurídico que se busca proteger es el patrimonial".*[146]

De acuerdo con lo anterior, indiscutiblemente la estafa informática contempla el patrimonio como uno de sus bienes jurídicos tutelados, inclusive desde su redacción antigua, denominada fraude informático, motivo por el cual la

---

[143] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 67.

[144] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 67-69. El resaltado no pertenece al original.

[145] LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 2ª ed. San José, 2020, p. 121.

[146] LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 2ª ed. San José, 2020, p. 119.

Sala Tercera de la Corte Suprema de Justicia, mediante resolución N° 2013-01258 de las 11:22 horas del 13-09-2013, al resolver un recurso de casación, en un asunto en el que se había condenado a una persona por haber cometido pluralidad de delitos de fraude informático, consideró que se podía aplicar el delito en su modalidad continuada, toda vez que el tipo penal tutelaba el bien jurídico patrimonio.

¿Es tan claro que el artículo 217 bis del CP tutele únicamente el bien jurídico patrimonio? La respuesta es no. Consideramos que, para un mejor análisis de la figura penal, surge la necesidad de cuestionar si podría ser más bien pluriofensiva, tomando en cuenta además del patrimonio, el bien jurídico de la autodeterminación informativa o algún otro. El artículo establece que, el sujeto activo mediante las conductas tipificadas, debe procurar u obtener un beneficio indebido para sí o para otro, ¿cuál puede ser ese otro beneficio indebido, independiente al patrimonio? El presente trabajo no es pretensioso en abarcar exhaustivamente el bien jurídico de la autodeterminación informativa, ello por no ser el tópico de la investigación, sin embargo, es necesario hacer referencia a él, para su debida comprensión y así, enfocarlo desde el punto de vista del delito de estafa informática, determinando si es o no tutelado por el numeral 217 bis del CP.

Dentro de la sociedad de la información en la cual nos desenvolvemos, los procesos de cambio devienen inevitables, por lo tanto, cobran vida nuevas conexiones o relaciones humanas, formas distintas de interacción. En ese sentido, en nuestro país, los artículos 23 y 24 de la Constitución Política regulan el derecho a la intimidad[147]. Los juristas HASSEMER y CHIRINO[148], señalan que de ambos

[147] *"ARTÍCULO 23.- El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley. ARTÍCULO 24.- Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento. Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y*

numerales parece reducirse el derecho a la intimidad a: “el domicilio”, las “comunicaciones” y “los documentos privados”, cuando en realidad el artículo 24, habla del derecho a la “libertad” relacionado con la intimidad. De tal manera, se abre la posibilidad para que pueda contemplarse la autodeterminación como una nueva dimensión de este derecho. Se da *“el delineamiento de una tutela de la intimidad en relación con la libertad, teniendo claro que aquella no se restringe ni a la “esfera íntima” o al “secreto de las comunicaciones”, sino que puede tener una interacción fundamental con la libertad, con la facultad del ciudadano de definir, programar y alcanzar su plan individual, y de participar y contribuir a la realización de un proyecto social”.* [149] Se deriva entonces que, concurre un punto de inflexión en cuanto al entendimiento que existía del derecho a la intimidad, antes del desarrollo de la sociedad de la información, en comparación al que podemos contemplar actualmente, y es en ese escenario en el que, la intimidad puede ser analizada o apreciada desde diversos enfoques, lo cual se integra en el concepto de autodeterminación informativa.

Es necesario mencionar que, el bien jurídico en cuestión surge del Tribunal Constitucional Alemán, en la sentencia sobre la Ley de Censos de 1983, mediante la cual le dio rango constitucional a la tutela del derecho a la autodeterminación informativa, en lo esencial es *“…la tutela del derecho del ciudadano a saber cuáles*

---

durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial. La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos. Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión. No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación. (Así reformado por el artículo 1° de la ley N.º 7607 de 29 de mayo de 1996)”.

[148] CHIRINO, Alfredo y HASSEMER, Winfried. *El derecho a la autodeterminación informativa y el reto del procesamiento automatizado de datos personales*. Editores del Puerto, 1997. p 97

[149] CHIRINO, Alfredo y HASSEMER, Winfried. *El derecho a la autodeterminación informativa y el reto del procesamiento automatizado de datos personales*. Editores del Puerto, 1997, p. 99.

datos suyos están siendo tratados, con qué fines, por cuáles personas, bajo qué circunstancias y con el fin de definir cuáles son los peligros que para su persona los mencionados tratamientos pueden tener […] tiene su punto de partida en la intimidad, pero significa más que ésta, es la tutela de áreas de libertad, de las áreas en las que un sujeto puede autodeterminarse, en la gestación y desarrollo de su plan de vida…"[150] El profesor Chirino agrega que: *"El nuevo papel de la intimidad, así planteado, rompe los viejos compartimentos estancos en que se desarrollaba la artificial escisión entre lo público y lo privado, entre lo personal y lo colectivo, entre lo íntimo y lo general, para abrir la puerta a la discusión sobre los espacios sociales donde se produce la interacción entre los ciudadanos para el alcance de objetivos comunes, haciendo ejercicio de nuevos matices de la libertad, potenciados por nuevas formas de comunicación. Esta nueva dimensión de la intimidad se manifiesta prontamente en el desarrollo jurídico de la década de los setenta y los ochenta, bajo la estructura jurídica del derecho a la autodeterminación informativa, con un profundo arraigo en principios tales como la dignidad humana, la libertad individual, la autodeterminación y la democracia, que antes de ser utilizados como puntos de sustentación vacíos y sin contenido, adquieren una nueva perspectiva en el Estado de Derecho…"*[151]

Dicho autor considera que, la autodeterminación informativa es un derecho fundamental que *"no es ningún nuevo derecho, sino que es la expresión de antiguos derechos como el derecho a la privacidad y al control del Estado, y a controlar que éste no limite los derechos de los ciudadanos de una manera insoportable, derechos que en alguna medida se han venido "contaminando" y reduciendo frente al avance constante y manifiesto de las tecnologías de la información y de la comunicación. Se trata de un derecho a saber y también un derecho a la transparencia del procesamiento de datos, el cual a su vez es una*

---

[150] CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica.* CONAMAJ, San José, 1997, p. 29.

[151] CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica.* CONAMAJ, San José, 1997, p. 16.

parte fundamental del concepto moderno de democracia…"[152] Si bien es cierto, la autodeterminación informativa nace como una especie de barrera a la actuación del Estado[153], se termina convirtiendo en un aspecto esencial y fundamental del diario vivir que tienen todas las personas frente a cualquier tipo de amenaza, indistintamente de la fuente de dónde emane el peligro, sea una persona física, jurídica, una institución de poder u otras.[154] El auge del procesamiento de datos en

---

[152] CHIRINO SÁNCHEZ, Alfredo. *Las Tecnologías de la información y el Proceso Penal. Análisis de una crisis anunciada*. En: Revista de la Asociación de Ciencias Penales de Costa Rica., año 9, n° 14, San José, 1997, p. 44.

[153] *"…El Tribunal Constitucional Alemán dedujo este derecho a la autodeterminación informativa al establecer una relación directa entre el derecho general a la personalidad y la dignidad del ser humano (artículo 2, párrafo 1 y el artículo 1 de la Ley Fundamental alemana). Esta línea interpretativa es clara si se entiende que este Tribunal meditó sobre la relación posible entre el control estatal de los datos de los ciudadanos y la posibilidad de una verdadera democracia compuesta por seres humanos que no tienen la posibilidad de autodeterminarse, muy especialmente en el ámbito del área más íntima de sus vidas […] El riesgo de la construcción de perfiles de personalidad, a través de los cuales es posible catalogar a los ciudadanos y a los grupos sociales, y tomar medidas de prevención social así como otras medidas de control está en la base misma de la reflexión del tribunal. Cuando éste afirma que no existen ya más datos sin interés, se está refiriendo al hecho de que para la construcción de perfiles de los ciudadanos cualquier detalle, característica, circunstancia o evento en su vida, que de cualquier otra manera pasaría desapercibido, es de una importancia decisiva para los fines del control estatal. Estas personas, así catalogadas, verían reducidas totalmente sus posibilidades de cumplir un papel social activo, ya que de muchas maneras se les negaría un amplio acceso a los medios sociales, ya sea porque se les ha catalogado como "grupos de riesgo", "asociales", "peligrosos", como "sospechosos", como "políticamente inconvenientes", como "enfermos", como "delincuentes" o bien como "deudores que no honran sus deudas" o incluso como "intelectuales comprometidos". El valor de este catálogo de características o de roles sociales tiene sentido en el contexto de una política estatal, y esto no es forma alguna una invención de un sueño descomunal y trágico perteneciente a una novela de fantasía, sino la trágica realidad a la que se enfrentan muchos ciudadanos en muchos lugares del mundo, en donde existen regímenes de carácter autoritario. El Tribunal Constitucional Federal alemán observó este peligro y declaró que en los casos donde los individuos estén totalmente subordinados a la colectividad y sometidos a ella, de tal manera que sus derechos individuales queden prácticamente sin ningún vigor o validez, nos encontramos en presencia de un sometimiento de carácter inconstitucional. Se configura de esta manera el "derecho a la autodeterminación informativa" como un derecho que pretende enfrentar el problema de "contaminación" a la que se enfrentan muchas libertades individuales consignadas en las Constituciones Políticas producto de los efectos provenientes de las nuevas tecnologías. Como un derecho fundamental de tercera generación es un derecho que tiene un valor de solidaridad, alcanzable por tanto a partir de un esfuerzo conjunto de la sociedad…"* CHIRINO SÁNCHEZ, Alfredo. *Las Tecnologías de la información y el Proceso Penal. Análisis de una crisis anunciada*. En: Revista de la Asociación de Ciencias Penales de Costa Rica., año 9, n° 14, San José, 1997, pp. 44 y 45.

[154] CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica.* CONAMAJ, San José, 1997, p. 10: *"…Como tantas otras herramientas de la historia, esta tecnología puede producir también una gran dimensión de beneficios, pero también una enorme cantidad de riesgos y peligros para el ciudadano, los cuales muchas veces pasan desapercibidos producto del carácter sutil e incruento y hasta atractivo de sus promesas. Estamos*

custodia del Estado y de particulares ha sido de tal magnitud en las últimas décadas *"…que la puerta al abuso está abierta de par en par…"*[155]

Continúa señalando el doctor Alfredo Chirino que *"…Este derecho no sólo tiene validez para el almacenamiento de los datos, sino también a todo lo largo del proceso de obtención de la información, de tal manera que la forma de almacenamiento de los datos (manual o electrónica) no tiene un verdadero papel fundamental. Tampoco tiene importancia la clasificación de los diversos tipos de datos ya que no existen datos que por sí mismos carezcan de interés. En un procesamiento de datos que permite la rápida comparación, unión, listado y análisis de todos los datos posibles de una persona, ya no tendría interés hablar de datos de mayor o menor importancia, o de datos de mayor o menor privacidad, ya que la construcción de perfiles de personalidad se realiza con la ayuda de todos los datos posibles, por lo que el ámbito de protección de este derecho se encuentra fuertemente caracterizado por la índole especial de los intereses en conflicto en el procesamiento de datos, principalmente del interés del ciudadano de tener control sobre quién y en qué forma, con cuáles objetivos y bajo qué circunstancias, tiene acceso a sus datos personales…"*[156] Nótese en ese sentido, la importancia en cuanto a la relación que existe entre la autodeterminación informativa y el uso indebido de datos de las personas, es un vínculo insoslayable, tal circunstancia nos acerca un poco a lo que prevé el delito de estafa informática,

---

dispuestos a canjear nuestra libertad a cambio de seguridad, aún cuando esta promesa sólo tenga efectos simbólicos. El canje no es obligatorio, pero lo aceptamos como necesario, ya que se presenta a nosotros como inevitable, es más, como el único medio, en una época en que imperan los medios y donde, como bien lo decía Albert Einstein, se da una gran confusión de fines. En el camino para obtener más "seguridad", comprometemos nuestra libertad. Abriendo la puerta a la tecnología, sin ninguna reflexión de sus problemas, la aceptamos como la panacea para los problemas de la humanidad. Si bien la tecnología puede producir muchos beneficios, también entrega en las manos de los organismos de control los hilos para la definición de nuestro presente y de nuestro futuro…"

[155] CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica*. San José, CR, CONAMAJ, 1997, p. 25.

[156] CHIRINO SÁNCHEZ, Alfredo. *Las tecnologías de la información y el proceso penal*. En: Nexos Costa Rica, Derecho y Legislación. Versión electrónica en: https://www.nexos.co.cr/archivo/perspectivas/tecnologias-informacion-proceso-penal.htm.

ya que dentro de sus elementos objetivos del tipo, se considera el concepto de "datos".

Como complemento de lo anterior, el autor Cristian Borghello, citado por el abogado especialista en delincuencia informática, Marcelo Temperini, señala que *"Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación".*[157]

Por su parte, el autor Gustavo Eduardo Aboso, señala, haciendo referencia a la autodeterminación informativa que: *"…el Tribunal Constitucional alemán ha reconocido de manera expresa este nuevo derecho a la integridad y la confidencialidad de los sistemas informáticos en dos sentencias cuyos objetos fueron, por un lado, la ley que autorizaba la recolección y el procesamiento de datos personales vinculados con aspectos económicos y financieros de las personas (BVerfGE 65, 1, 43); por el otro, la aplicación del registro y tratamiento de datos personales a los fines de la investigación penal (BVerfGE 115, 320), En (sic) ambos casos, ese tribunal constitucional fue moldeando el sentido y el alcance de este nuevo derecho de autodeterminación informativa que básicamente reconoce y ampara constitucionalmente el dominio sobre la disposición de los datos individuales o individualizables de personas, cuyo ejercicio impone límites precisos a la autoridad pública sobre su uso y aplicación…"*[158]

Vale referir que, en América Latina, en esa coyuntura de la discusión del procesamiento de datos, surge necesariamente la figura del "*habeas data*", la cual deriva del "*habeas corpus*", que pretende proteger jurídicamente el derecho de las

[157] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características.* En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 50.

[158] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 40.

personas de acceder a las informaciones personales contenidas en registros magnéticos y manuales, con la intención de que puedan ser revisadas, y que en caso que, pueden representar un perjuicio, puedan ser corregidas o eliminadas. El concepto de "*habeas data*" es posible vincularlo con el de "libertad informática" que, de acuerdo con el autor Frossini, citado por Chirino, es *"…el derecho de conocimiento y de autodecisión sobre los datos personales propios…"*, sin embargo, ese poder sobre los datos no es absoluto ni definitivo, ya que el derecho radica en que las personas estén informadas del procesamiento de datos y los fines que se quieran alcanzar, por lo tanto, lo esencial resulta ser la "autodecisión" o la "autodeterminación" de la persona, garantizando consecuentemente su participación frente a un procesamiento de datos personales, evitando que sea invisible y por ende un mero objeto del entorno informativo.[159]

Tabla 5. Principios de la autodeterminación informativa

Algunos principios del derecho a la autodeterminación informativa[160]	
Principios	**Significado**
Libertad de decisión del afectado	La persona afectada tiene libertad de decidir sobre el fin u objetivo del procesamiento de datos personales.
Transparencia sobre el tipo, dimensión y fines del procesamiento de datos	La persona afectada debe conocer quién y con qué fines realiza un tratamiento de sus datos personales.
Sujeción al fin del procesamiento	La persona afectada se sujeta al fin del procesamiento para el cual dio su consentimiento, a partir de un conocimiento que se le ha facilitado sobre tal fin y objetivo.
Separación de poderes informativos	Debe existir una división técnica y organizacional entre el procesamiento de datos frente a otros fines de utilización de los datos personales.
Prohibición del	Prohibición de almacenar datos con el fin de facilitar la

[159] CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica.* CONAMAJ, San José, 1997, p. 20.

[160] CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica.* CONAMAJ, San José, 1997, p. 43.

procesamiento de datos “a beneficio de inventario”	verificación de un tratamiento de datos no autorizado posterior, y la prohibición de la construcción de perfiles a partir del procesamiento de datos personales.
Derecho “al olvido”	Reglas de destrucción de datos personales una vez cumplido el fin para el que fueron recopilados.
Aseguramiento técnico	Materialización de principios jurídicos encaminados a tutelar a la persona frente al procesamiento de sus datos personales.
Control del procesamiento	Que los lugares de procesamiento de datos independientes sean controlados.

A lo anterior se le debe agregar que, en el mundo de la seguridad de la información, existen tres pilares fundamentales o básicos que se intentan resguardar:

“-La integridad de la información es la característica que hace que su contenido permanezca inalterado, a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema. -La disponibilidad u operatividad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la información se mantenga correctamente almacenada, con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria. -La privacidad o confidencialidad de la información es la necesidad de que solo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos perjuicios a su dueño...”[161]

Nuestra Sala Constitucional considera que la autodeterminación informativa deriva del numeral 24 de la Constitución Política, y lo ha entendido como *“…el*

[161] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características.* En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 51.

derecho de toda persona a tener conocimiento de los datos que sobre ella consten en un registro o archivo de cualquier naturaleza, así como del uso que se dará a dicha información. Asimismo, se ha sostenido que el derecho mencionado faculta a la persona a actualizar, rectificar, o eliminar aquella información que conste en una base de datos pública o privada, que no sea correcta o exacta, así como a que ésta no sea empleada para un fin diverso al que legítimamente debería cumplir, o para el cual se dio la información, salvo que, en este último supuesto, medie el consentimiento expreso del otorgante…"[162]

Es necesario referir que, en Costa Rica se cuenta con la ley N° 8968 denominada *"Protección de la persona frente al tratamiento de sus datos personales"*[163], del 07 de julio de 2011, publicada en La Gaceta N° 170 del 05 de septiembre de 2011, cuyo objetivo y fin se establecen en el artículo 1, señala: *"Esta ley es de orden público y tiene como objetivo garantizar* ***a cualquier persona, independientemente de su nacionalidad, residencia o domicilio****, el respeto a sus derechos fundamentales, concretamente,* ***su derecho a la autodeterminación informativa*** *en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes."*[164] Asimismo, en el artículo 4, se establece que dicho derecho *"abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales*".

De acuerdo con lo anterior, es claro que sí se ha reconocido en nuestro ordenamiento jurídico la tutela del derecho a la autodeterminación informativa. Y

---

[162] SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA, resolución N° 2014-003192 del 07-03-14 de las 09:05 h.

[163] Sobre dicha Ley refiere la profesional en informática Marta Eunice Calderón Campos: *"…no es perfecta, pero constituye un primer esfuerzo para crear conciencia en la sociedad costarricense de la importancia de proteger los datos personales."* Ver en CALDERÓN CAMPOS, Marta Eunice. *Marco jurídico de la profesión informática en Costa Rica*. Editorial Universidad de Costa Rica (UCR), Costa Rica, 1ª ed. 2018, p. 35.

[164] El resaltado no corresponde al original.

es que *"…la libertad informativa es una libertad tan esencial como la libertad de tránsito o de movimiento, muy especialmente en una sociedad que pone un énfasis tan contundente en el tráfago de datos personales. No en vano se ha dicho, que hay una relación de proporcionalidad directa entre el grado de democracia de un país y el número de informaciones que circulan en ella. En esa misma medida el grado de democracia puede verse en peligro si esas informaciones son utilizadas para reducir al ciudadano a un mero objeto de este trueque…"*[165]

Analizado todo lo anterior, cabe preguntarse si es posible que la estafa informática con la redacción actual, tutele el bien jurídico de la autodeterminación informativa de las personas o algún otro derecho[166], ello sumado a que indiscutiblemente es un delito que *prima facie*, protege el bien jurídico del patrimonio. Propiamente el artículo 217 bis del CP establece como requisitos objetivos del tipo penal que la conducta del sujeto activo tiene que ser llevada a cabo "…*mediante el uso de datos falsos o incompletos, el uso indebido de datos,*

---

[165] CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica*. San José, CR, CONAMAJ, 1997, p. 58.

[166] Ver LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 1ª ed. San José, 2011, p. 124. Señala con respecto al bien jurídico tutelado por el extinto delito de fraude informático previsto en el numeral 217 bis del Código Penal, al considerarlo como un tipo penal de peligro abstracto: *"¿Cuál es el bien jurídico que se protege?, remitiéndose a que la acción penal se ejerce contra los datos procesados en un sistema, como se explicó anteriormente y que el daño patrimonial no es necesario que se configure.* ***Sólo queda entender que el bien jurídico protegido deba ser la integridad de los datos en un sistema****, de esta manera la información (la información está compuesta de datos) procesada por medios informáticos como tal, se le ha tenido que brindar la protección necesaria desde el ámbito penal como un bien jurídico fundamental de la cibersociedad costarricense…"* Ver LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 2ª ed. San José, 2020, pp. 119-120, con respecto a la estafa informática: *"En primera instancia, el bien jurídico que se busca proteger es el patrimonial, pero sucede un aspecto muy interesante en este tipo penal: no contempla una acción acabada del delito con el simple hecho de tener la intención de procurar u obtener un beneficio patrimonial, ya que el delito se configura como de peligro abstracto al no requerir un resultado concreto para que se hable de uno consumado. Al ser así, no es necesario causar el perjuicio sobre el sujeto pasivo, entonces es posible no afectar el patrimonio de un sujeto pasivo y de igual manera cometer el delito […] remitiéndose a que la acción penal se ejerce contra los datos procesados en un sistema […] y que no es necesario que se configure el daño patrimonial,* ***nos queda entender que el bien jurídico protegido debe ser la integridad de los datos de un sistema****. De esta manera, la información procesada (la cual está compuesta de datos) por medios informáticos como tal ha debido ser protegida desde el ámbito penal como un bien jurídico fundamental de la cibersociedad costarricense…"* (el resaltado no corresponde al original).

programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro…"

Para comprender si la autodeterminación informativa es tutelada en dicho numeral, se debe definir qué se entiende por "datos", concepto que vale mencionar es distinto al de "información"[167]: *"…Es responsabilidad de los dispositivos de entrada/salida o de los programas codificar y decodificar (interpretar un patrón de bits[168] como texto, número, audio y video). Los datos, a diferencia de la información, son utilizados por diversos métodos para comprimir la información a fin de permitir una transmisión o almacenamiento más eficaces. Aunque el procesador de la computadora hace distinción vital de la información entre los programas y los datos, la memoria y muchas otras partes de la computadora no la hace. Ambos son registrados temporalmente según la instrucción que se le dé. Es como un pedazo de papel que no sabe ni le importa lo que se escriba en él: un poema de amor, las cuentas del banco o instrucciones para un amigo. Es lo mismo que la memoria de la computadora. Sólo el procesador reconoce la diferencia entre datos e información de cualquier programa. Para la memoria de la computadora, y también para los dispositivos de entrada y salida (E/S) y almacenamiento en disco, un programa es solamente más datos, más información que debe ser almacenada, movida o manipulada. La*

---

[167] Ver CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 37: *"Información" es, según algunos, el contenido informativo del dato. Lo que caracteriza al dato es su carácter formal, mientras que la información constituye la sustancia intelectual"*.

[168] Ver CEDANO OLVERA, Marco Alfredo, CEDANO RODRÍGUEZ, José Antonio, RUBIO GONZÁLEZ, José Antonio, y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010, p. 72: *"¿Qué es un bit? Es la mínima pulsación electrónica que recibe una computadora (bit, binary digit: dígito binario); es decir, es la mínima cantidad de información (datos) que recibe una computadora y puede ser ya sea 0 o 1 y representa el estado de un dispositivo que puede tomar uno de dos estados. Un foco puede estar apagado o encendido. El significado o representación es la siguiente: 1= encendido y 0= apagado. Un interruptor electrónico puede representar un bit. Actualmente las computadoras utilizan varios dispositivos binarios de dos estados para almacenar datos."*

cantidad de información de un mensaje puede ser entendida como el número de símbolos posibles que representan el mensaje. Los símbolos que representan el mensaje no son más que datos significativos. En su concepto elemental, la información es un mensaje con un contenido determinado emitido por una persona hacia otra y, como tal, representa un papel primordial en el proceso de la comunicación, a la vez que posee una evidente función social. A diferencia de los datos, la información tiene significado para quien la recibe; por eso, los seres humanos siempre han tenido la necesidad de cambiar entre sí información que luego transforman en acciones. La información es, entonces, conocimientos basados en los datos a los cuales, mediante un procesamiento, se les ha dado significado, propósito y utilidad…"[169]

El Convenio sobre la Ciberdelincuencia, Budapest (2001), indica en el artículo 1, inciso b) que *"por datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función."*

A partir de lo anterior podríamos decir que los datos se presentan de formas distintas, tales como[170]:

- Audio
- Imágenes
- Números
- Texto
- Video

[169] CEDANO OLVERA, Marco Alfredo, CEDANO RODRÍGUEZ, José Antonio, RUBIO GONZÁLEZ, José Antonio, y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010, p. 70.

[170] CEDANO OLVERA, Marco Alfredo; CEDANO RODRÍGUEZ, José Antonio; RUBIO GONZÁLEZ, José Antonio; y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010, p. 71.

Nótese entonces que el concepto de "datos" desde el punto de vista informático, es sumamente amplio. El jurista Francisco Castillo refiere que *"...Datos son, al lado de "informaciones", "programas" y "procesamiento de datos", el objeto material de la acción del art. 217 bis Cód. pen., así como el concepto de "hechos" son el objeto material de la acción en el art. 216 Cód. pen. […] Por "datos" debe entenderse una palabra, una imagen, un número o sonido convertido en una serie de "bit" o sea digitalizado […] Al lado de los datos de la computadora propiamente dicha, son también datos, si puede leerlos la computadora, escritos, fotografías o palabras, lo cual es posible a través de ciertas formas de "scanner" […] Hay una definición de datos en el § 202 a StGB alemán (Ausspähen von Daten=espionaje de datos), que dice lo siguiente: "Datos, en el sentido del párrafo I, son solamente aquellos, que son almacenados o transmitidos de manera electrónica, magnética o de manera no inmediatamente perceptible por los sentidos […] La codificación de la información es un elemento constitutivo del concepto de datos. No hay ninguna restricción respecto a determinada clase de codificación. Por ejemplo, en la codificación digital que se realiza por medio del código binario pueden codificarse expresiones escritas y expresiones orales y otras características de un ser humano. Lo que guarda el inicio del proceso puede ser una expresión escrita ("password"), puede ser una palabra de determinada persona (proceso que se inicia con la voz de una persona) o puede ser una característica individual (por ejemplo, la huella digital, el color del iris de los ojos de una persona)."*[171]

A la luz del numeral 217 bis del CP, el profesor Castillo considera que el "dato" está caracterizado por lo siguiente[172]:

- A diferencia del concepto de "hechos" de la estafa convencional, el concepto de "dato", no requiere ser objeto de prueba.

---

[171] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 32-35.

[172] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 36 y 37.

- No se demanda que el “dato” esté protegido de determinada forma.
- No se exige que el “dato” sea producto o resultado del proceso realizado por un computador.
- La “información” puede tener como contenido “datos”.
- Pueden ser objeto de juicios de valor.
- Conforme al principio de legalidad, no existe una limitación del contenido de datos a hechos de relevancia patrimonial.
- El tipo penal integra una limitación del posible contenido de los datos, reflejado en los siguientes adjetivos: *“uso de datos falsos o incompletos”*, *“uso indebido de datos”*, o el requisito de que el autor del delito produzca con la manipulación de datos un daño patrimonial.

Según el profesor Francisco Castillo, la utilización de un programa falso, encaja perfectamente en el tipo penal, toda vez que un programa se compone de datos, en ese sentido: *“…falso es un programa cuando la (sic) órdenes de trabajo establecidas por medio de datos llevan a un resultado que objetivamente se apartan del resultado a que se llegaría si no hubiera habido la manipulación del sistema de procesamiento de datos…”*[173]

Cuando el sujeto activo de la conducta hace uso debido de: audios, imágenes, números, texto o video; programas o información, dentro de alguna operación informática, al actuar de manera lícita no estaría incurriendo en el delito de estafa informática. Castillo lleva razón al decir que *“…“Uso debido” es sinónimo de actuar con derecho…”* pudiendo provenir ese uso debido de diversas fuentes, entre ellas: leyes, contratos, o autorización expresa o tácita del derecho-

[173] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 93 y 94.

habiente.[174] A *contrario sensu*, cuando el sujeto activo hace uso indebido de datos, ya sea ingresando a la plataforma electrónica la información bancaria y realiza transacciones sin la autorización respectiva, o simplemente utiliza la clave confidencial en un sistema informático sin mediar consentimiento, y realiza retiros de dinero, podríamos afirmar que efectivamente se vulnera el derecho de la autodeterminación informática[175], toda vez que se utilizaron datos personales de carácter restringidos[176], ya que son de interés únicamente del titular.

Mediante una interpretación gramatical o literal[177], del numeral 217 bis del CP, se detecta que el sujeto activo tiene que realizar el comportamiento ya sea,

---

[174] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 97.

[175] Ver en ese sentido CALDERÓN CAMPOS, Marta Eunice. *Marco jurídico de la profesión informática en Costa Rica*. Editorial Universidad de Costa Rica (UCR), Costa Rica, 1ª ed. 2018, pp. 32 y 33. Cuando analiza la resolución de la Sala Constitucional N° 2015-7357 de las 09:15 h del 22-05-2015: *"En esta sentencia se hace referencia a otras anteriores, entre ellas la 1779-2013 y 18952-2014, en las cuales la Sala Constitucional indica que el correo electrónico y los documentos electrónicos almacenados en la computadora utilizada por una persona están protegidos por el derecho fundamental al secreto de las comunicaciones y el control de ellos debe realizarse con las garantías establecidas por la Constitución Política. Además, la garantía del derecho es independiente de quien sea el dueño de la computadora."* Nótese que, si el ingreso a un correo electrónico es protegido, de igual manera lo es el ingreso a una base de datos en donde se encuentra información bancaria confidencial. La Sala Constitucional en la resolución analizada por la autora, mencionó: *"…si la Directora Ejecutiva del Patronato Nacional de Ciegos ordenó el bloqueo de las cuentas de correo electrónicas de los recurrentes y* ***se impuso al menos del título y fecha del correo, produjo con ello una amenaza cierta e inminente a sus derechos fundamentales, lo que también facilita que cualquier persona ajena, se impusiera del contenido de los mensajes y documentos privados sin el consentimiento de los agraviados, lo que supone una violación al artículo 24 de la Constitución Política****."* (el resaltado no corresponde al original).

[176] La ley N° 8968 denominada *"Protección de la persona frente al tratamiento de sus datos personales"*, en el artículo 4 incisos b) y d), define respectivamente los siguientes conceptos: *"datos personales"* como *"cualquier dato relativo a una persona física identificada o identificable"*; y *"datos personales de acceso restringido"* como: *"los que, aun formando parte de registros de acceso público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública."*

[177] Ver GARCÍA FIGUEROA, Alfonso; GASCÓN ABELLÁN, Marina; MARCILLA CÓRDOBA, Gema; PRIETO SANCHÍS, LUIS. *Argumentación jurídica*. Tirant lo Blanch. Valencia. 2014, pp. 271 y 272: *"Así, en el Derecho penal, donde el valor de la certeza y previsibilidad adquiere una importancia crucial para la garantía de la libertad y los derechos, se impone una interpretación literal o estricta de la ley, en detrimento de cualquier otro tipo de interpretación extensiva. Esta es precisamente una de las razones por las que en los sistemas que quieran reclamarse mínimamente garantistas se prohíbe la analogía en el derecho penal y en caso de lagunas habrá que argumentar conforme al argumento a contrario. Y en general puede decirse que en un ordenamiento que tome en serio el principio de legalidad, los argumentos que apelen al tenor literal de la ley o a la voluntad del*

con una finalidad de procurar u obtener un beneficio patrimonial o un beneficio indebido. Nótese que la persona legisladora, después de “beneficio patrimonial”, introdujo en el texto la letra “o” disyuntiva, admite, por lo tanto, que no se tiene únicamente una finalidad patrimonial. En ese sentido señala el abogado costarricense Ricardo Salas: *"Asimismo, debe repararse en que por la redacción concerniente al dolo específico, hay una diferencia importante entre este y el de la estafa común. En el artículo 216 se dice que es "...para obtener una (sic) beneficio patrimonial antijurídico para sí o para un tercero..."; en tanto que en el 217 bis se dice que es para procurar u obtener "...un beneficio patrimonial o indebido para sí o para otro" (subrayado suplido). En otras palabras, el beneficio buscado no siempre tiene que ser patrimonial, sino que basta con que sea indebido, lo cual abre el arco de posibilidades a todas aquellas situaciones provechosas contrarias al Ordenamiento Jurídico, sin necesidad de que sea de índole patrimonial."*[178] Por esa apertura es que, podría considerarse la autodeterminación informativa como bien jurídico tutelado, toda vez que en el fondo, la estafa informática, termina sancionando a quien utilice datos de forma indebida, en una de sus modalidades de comisión. De igual manera, cuando se hace uso de datos falsos o incompletos, se termina afectando la información del sujeto pasivo, aquella que está resguardada en instituciones financieras, por ejemplo. A pesar de lo anterior, es necesario analizar cada caso en concreto, para determinar, si se afecta o no dicho bien jurídico. Por la redacción del artículo 217 bis del CP, también cabe la posibilidad que, en aquellas formas de comisión del hecho mediante datos falsos e incompletos, se vulnere la “integridad de los datos de un sistema”, tal y como lo refiere el autor Roberto Lemaître.

El profesor Francisco Castillo señala que, el patrimonio en su expresión especializada de datos y programas, es el único bien jurídico tutelado por el numeral 217 bis del CP, sin embargo, no comparto del todo dicha posición, puesto

---

legislador real (o sea, el argumento del lenguaje común y el subjetivo o psicológico) prevalecen prima facie sobre los demás…”

[178] SALAS PORRAS, Ricardo. *Derecho penal especial*. Editorial Investigaciones Jurídicas S.A, 1ª ed. San José, 2019, p. 161.

que el artículo en sentido estricto no es una estafa, y en el fondo si bien tutela el patrimonio, también deja abierta la posibilidad de resguardar otros bienes jurídicos, como la autodeterminación informativa, la cual considero de gran relevancia en la actualidad[179].

El autor Roberto Lemaître, advierte con respecto a la estafa informática: *"El problema que surge en este tipo penal es cuando bandas organizadas o personas individuales son detenidas con la información que han sustraído con claridad para ejecutar una estafa. Pensemos en los casos donde estas personas han tomado datos por medio de skimmers en un cajero y han copiado la información de cientos de clientes; sin embargo, todavía no han utilizado ni un solo dato recolectado en un sistema de información. En este caso nos encontramos ante la imposibilidad de poder imputarles el delito; este es un vacío que presenta nuestra normativa."*[180]

En realidad, si considerásemos la autodeterminación informativa, como bien jurídico tutelado por la estafa informática, dicha actuación en coautoría tal cual la ejemplifica el autor, no necesariamente se encuentra despenalizada, ya que desde el momento en que los sujetos activos extraen la información bancaria de las víctimas sin su consentimiento, mediante los dispositivos denominados *"skimmers"* (artificio tecnológico), podría interpretarse que ya están haciendo uso en sentido

---

[179] Ver GARCÍA FIGUEROA, Alfonso; GASCÓN ABELLÁN, Marina; MARCILLA CÓRDOBA, Gema; PRIETO SANCHÍS, LUIS. *Argumentación jurídica*. Tirant lo Blanch. Valencia. 2014, p. 249: *"**Problemas de funcionalidad**. Tampoco en este caso se trata de problemas interpretativos stricto sensu, sino de problemas teleológico-valorativos de aplicación de la ley que surgen cuando una disposición, cuyo significado no ofrece dudas ni es contradictorio, provoca alguna perplejidad en su aplicación literal a un caso específico, bien porque se considera que éste es excepcional, bien porque han cambiado las circunstancias (por ejemplo, cambios tecnológicos o científicos no imaginados por el legislador) o las valoraciones sociales. La duda que en estos casos se plantea es si aplicar la disposición en su significado inmediato o, por el contrario, corregir ese significado para adaptarlo a las nuevas circunstancias. En general, los avances científicos y tecnológicos plantean constantemente problemas de funcionalidad al Derecho, que ha de adaptarse a la nueva situación por vía legislativa, pero también, y entretanto esto no ocurra, por vía interpretativa. Y piénsese también en el reto que supone para el Derecho el vertiginoso desarrollo de la tecnología informática, un Derecho no pensado para regular los problemas que surgen como consecuencia de esos nuevos avances. Pero esto es también lo que sucede con el concepto de matrimonio y con numerosas instituciones del derecho de familia, que deben ser adaptadas para dar cuenta de las concepciones actualmente vigentes."*

[180] LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 2ª ed. San José, 2020, pp. 119 y 120.

amplio de esos datos de una manera indebida, toda vez que desde que se inicia el traslado de esos datos de un dispositivo de almacenamiento a otro (de la tarjeta al *"skimmer"*), se empezó a hacer uso de esos datos que antes no se tenían, por lo tanto, atendiendo el caso de ejemplo, la información privada de las víctimas se vio vulnerada y los imputados obtuvieron un beneficio indebido para sí, en consecuencia: **1)** lesionaron el bien jurídico de la autodeterminación informativa y **2)** al tratarse de datos financieros ponen en riesgo el bien jurídico patrimonio. Si bien se tendría que analizar el caso en concreto, podríamos estar ante una tentativa de estafa informática, ya que el tipo penal debería entenderse a nuestro criterio como de resultado[181], siempre y cuando, la razón por la cual finalmente no influyeron en el sistema informático mediante la utilización de esos datos, obedeció a una causa ajena a la voluntad del agente.

Se podría considerar que, de acuerdo al caso expuesto, se cumplen algunos de los elementos objetivos del tipo penal 217 bis del CP, ya que los imputados sí hicieron uso indebido de los datos de las víctimas (trasladarlos y almacenarlos en el *skimmer*), en evidentes actos de ejecución, con la finalidad de influir en un sistema informático de datos, procurando obtener un beneficio indebido para sí o para otro, puesto que sería ilógico considerar que éstas personas que mediante la utilización de un *skimmer* en un cajero automático, con el cual copiaron la información de las tarjetas de cientos de clientes, se hicieran de esos datos valiosos, sin pensar en un beneficio ulterior, eminentemente indebido, el cual con una probabilidad lindante en seguridad sería de carácter patrimonial.

---

[181] Ver en ese sentido CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 131: *"El delito de estafa informática es un delito de resultado, que se consuma cuando se produce (total o parcialmente) el perjuicio patrimonial"*. Sin embargo, el mismo autor en la obra CASTILLO GONZÁLEZ, Francisco. *La estafa informática de "Lege lata" y de "lege ferenda"*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 298, parece que lo considera de peligro, al afirmar: *"El texto vigente de la estafa informática del art. 217 bis Cód. pen.* ***no establece como requisito para la consumación la causación de un perjuicio patrimonial****." (el subrayado y resaltado no corresponde al original)*. Creemos que esta última posición del autor no es la correcta, toda vez que, ante la redacción del tipo penal, en el cual se considera "procurar" u "obtener" un beneficio patrimonial o indebido, debemos entender que el delito se consuma cuando el sujeto activo obtuvo el beneficio patrimonial.

Lo que sí es cierto, es que, si los imputados son detenidos sin haber utilizado en un sistema informático esos datos, de manera que no se influyó en el sistema informático y por ende no se obtuvo el beneficio patrimonial indebido, queda abierta la posibilidad de una tentativa, incluso de un desistimiento voluntario. Vale referir en ese sentido que *"para los efectos de aplicación del artículo 217 bis Cód. pen. solamente son relevantes los concretos procesos de un sistema de procesamiento de datos que lleven a un resultado patrimonial lesivo"*[182]. De igual manera no tenemos que dejar de lado la posibilidad de subsumir dicha conducta en el artículo 196 bis del CP, denominada *"violación de datos personales"*[183], por lo que no resulta del todo cierto, que la conducta esté despenalizada.

Ahora bien, hilando delgado, incluso podría afirmarse que se consumó la estafa informática, tanto en sus elementos objetivos como subjetivos, desde que los imputados colocaron el *skimmer* en el cajero automático, las víctimas introdujeron las tarjetas en él y se creó la copia de información bancaria de cientos de clientes en dicho aparato informático, puesto que, dependiendo de las

---

[182] CASTILLO GONZÁLEZ, Francisco. *La estafa informática de "Lege lata" y de "lege ferenda"*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 282.

[183] ***"Código Penal. Artículo 196 bis.-Violación de datos personales.*** *Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos. La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:* ***a)*** *Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.* ***b)*** *La información vulnerada corresponda a un menor de edad o incapaz.* ***c)*** *Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona. No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley. Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley." (Así adicionado por Ley N° 8148 de 24 de octubre del 2001 y posteriormente reformado en la forma indicada por el artículo 1° de la ley N° 9135 del 24 de abril de 2013)".*

características que ostente ese artificio tecnológico (en tanto existen diferentes tipos), podría ser considerado en sí mismo un sistema automatizado de información, toda vez que entre sus funciones se encuentra la entrada de datos, es decir, se le puede ingresar información[184], además, cuenta con una unidad central de proceso, en la cual se crea una lista de elementos de cientos de clientes, característica clásica en el procesamiento de datos desde un punto de vista informático; además, está integrado por una memoria, y esos datos copiados, pueden ser extraídos del *skimmer,* por lo que tiene una función de salida de datos, que se presenta cuando los imputados extraen de dicho aparato los datos o elementos almacenados de los clientes y los ingresan en otros dispositivos, como los plásticos genéricos de tarjetas u otro computador.

Es decir, siguiendo con el ejemplo, los sujetos activos, no solo habrían incurrido en el uso indebido de datos, sino que, si entendemos que el *skimmer* es en sí, un sistema automatizado de información, se influyó o incidió en ese sistema de procesamiento de datos, con lo que obtuvieron un beneficio indebido, ya que se hicieron de los datos bancarios de las víctimas sin autorización, conducta que cumple con los requisitos de tipicidad exigidos por el artículo 217 bis del CP, en su primer párrafo.

Y es que, ese elemento descriptivo del tipo penal, sea el *"sistema automatizado de datos"*, puede ser integrado por un aparato informático desde muy simple en su procesamiento de datos hasta muy complejo, siempre y cuando tenga la capacidad de procesamiento de datos, como lo podría el *skimmer*. En consecuencia, no necesariamente el caso expuesto sería atípico del delito de estafa informática, sino que dependerá de las circunstancias que se presenten, lo que exige de la persona operadora del derecho un análisis acucioso, en tanto nos enfrentamos a criminalidad no convencional, que representa un reto intelectual para acreditar o descartar la subsunción de la conducta en el tipo penal.

---

[184] Proceso denominado función identidad, que consiste en una operación matemática que copia la información de la fuente, en este caso la tarjeta bancaria, al dispositivo *skimmer*. Ver sitio web: https://www.funciones.xyz/funcion-identidad/. Consulta realizada el 27 de julio del 2021.

Es necesario indicar que el delito de estafa informática tutela el patrimonio como principal bien jurídico, mientras tanto, el delito de violación de datos personales previsto en el artículo 196 bis del Código Penal, resguarda específicamente los bienes jurídicos de la intimidad, privacidad de datos e incluso la misma autodeterminación informativa. De acuerdo a lo anterior, en caso de concurrir una misma conducta en ambos tipos penales, deberá atenderse el caso en concreto para determinar cuál tipo penal desplaza al otro, sin embargo, *prima facie* se puede decir que, predominará por especialidad la estafa informática, siempre y cuando el dolo del agente sea obtener un beneficio patrimonial. En caso de que el sujeto activo pretenda una finalidad distinta a la patrimonial y siendo que compromete la autodeterminación informativa de la víctima, deberá predominar el artículo 196 bis del CP.

Evidentemente, al analizar el tipo penal de estafa informática, se infiere que nos encontramos ante un tipo penal abierto[185] y pluriofensivo, es decir, que por su redacción, tutela no únicamente el patrimonio, sino que también protege la autodeterminación informativa e incluso la integridad de los datos de un sistema, análisis que debe ser casuístico; situación que inclusive tal y como se verá en el tercer capítulo, queda confirmada con los fines que quiso alcanzar la persona legisladora al momento de redactar el artículo. Nótese que el delito de estafa informática en determinados supuestos, pero principalmente en la modalidad de

[185] Ver CALDERÓN CHINCHILLA, Rosaura. *El principio de legalidad ¿muro de contención o límite difuso para la interpretación de la teoría del delito en C.R.?* Editorial Investigaciones Jurídicas S.A., 2ª ed. San José, 2018, pp. 51 y 52: *"**iv. LEX CERTA O MANIFESTA**. Exige la tipicidad de la conducta, la taxatividad en la enunciación de los tipos penales y la claridad en la descripción, con el fin de evitar la ambigüedad en el uso del idioma eliminando los tipos penales abiertos, las leyes penales en blanco, los conceptos jurídicos indeterminados, las cláusulas generales, los elementos normativos del tipo, y todo aquello que genere inseguridad respecto de la conducta punible o la sanción a imponer. En el marco del surgimiento del Derecho Penal Moderno o el Derecho Penal del Riesgo que aboga, justamente, por la expansión del ius puniendi estatal a través del uso de –entre otros- estos mecanismos, se hace necesario que se denuncie la ilegitimidad constitucional de estas expresiones. Pero, a pesar de que mantenemos que con ellas –sin excepción alguna- se da la violación al principio de legalidad, la Sala Constitucional ha tenido oportunidad de aceptar matizadamente algunas de esas prácticas […] **Sin que haya llegado a avalar el uso de tipos abiertos respecto de los que ha emitido la declaratoria de inconstitucionalidades: Sala Constitucional, votos N° 1877-90; N° 447-91; N° 2000-9249 y ha indicado: "Estos tipos en tanto entrañan un grave peligro de arbitrariedad, lesionan abiertamente el principio de legalidad de los delitos" (votos N° 490-94 y N° 2000-11524)**."* El resaltado no corresponde al original.

comisión de uso indebido de datos, es una figura que tutela la autodeterminación informativa, ya que se utilizan datos de una víctima sin su consentimiento, información que además de privada es valiosa, y que el sujeto activo se hizo de ella por algún medio, *ergo*, los derechos de privacidad e intimidad se verán lesionados, integrados ambos en el derecho ya expuesto de la autodeterminación informativa. El autor Gustavo Eduardo Aboso, en su libro, propiamente en el capítulo VIII, titulado *"Delitos contra la propiedad (I): Estafa y fraudes informáticos"*, señala lo siguiente: *"...junto al objeto de protección mencionado, esto es, el patrimonio, confluyen otros intereses penalmente tutelados que se identifican con la integridad, el correcto funcionamiento y la facultad de disposición de datos, es decir, los tipos penales que analizaremos […] se solapan en muchos sentidos desde el punto de vista del objeto penalmente tutelado, al extremo de constituir "tipos penales conglomerantes" en razón de la pluralidad de intereses protegidos en juego."* [186]

Tal y como lo hemos venido señalando, existe alguna corriente doctrinaria que considera que la integridad, funcionalidad y confidencialidad de los sistemas informáticos pueden ser nuevos bienes jurídicos para el Derecho Penal, siendo necesario tutelar, comportamientos lesivos que afectan esa funcionalidad sistémica, es decir, una protección de los sistemas telemáticos en la coyuntura que implica la sociedad tecnológica en la cual nos desenvolvemos. Esa es una valoración importante a tomar en cuenta, precisamente porque el delito de estafa informática se encuentra directamente relacionado con sistemas informáticos en los cuales se utilizan datos de forma indebida.[187]

---

[186] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 299.

[187] Ver ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, pp.37-40: *"…**se** comienza a hablar en los círculos especializados sobre la necesidad de tutelar la propia integridad y funcionalidad de los sistemas telemáticos, al mismo tiempo de la facultad de disposición de los datos almacenados por particulares, empresas y gobierno. La decisión marco 2005/222/JI del Consejo de la Unión Europea ha dado un paso adelante en la tutela de manera autónoma de la integridad y la confidencialidad de los sistemas informáticos. Surge una vez más la necesidad de*

En ese mismo sentido, el abogado Marcelo Temperini, señala que existe una posición doctrinaria que considera como nuevo bien jurídico a tutelar en los delitos informáticos, la información. Respalda su dicho, remitiéndose a palabras del Dr. Santiago Acurio Del Pino: *"Podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan… Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere*"[188]. De igual manera, indica dicho autor que una de las legislaciones sobre delitos informáticos más modernas en el continente, es la de Colombia, la cual considera en el artículo 1 de la ley 1273 de 2009, a la

---

estrechar los lazos de cooperación internacionales frente a manifestaciones cada vez más frecuentes de ataques informáticos contra la integridad, la seguridad, la funcionalidad y la confidencialidad de los sistemas telemáticos. Esta dependencia de la moderna sociedad de los avances tecnológicos obliga a las autoridades nacionales a adoptar medidas sancionatorias contra esta peculiar forma de agresión. En consecuencia, esta decisión europea insta a los países miembros a armonizar sus legislaciones nacionales con el propósito de crear un frente común contra los accesos ilegítimos a los sistemas informáticos. Esta normativa comunitaria europea tuvo como eje central los accesos ilegales, es decir, no autorizados al conjunto o una parte de un sistema de información (art. 2) y las intromisiones no autorizadas en los sistemas y los datos (art. 3), especialmente el llamado "sabotaje o daño informático" […] Esta decisión marco determinó reformas en las legislaciones penales de los países miembros para armonizar la legislación penal en la lucha contra la cibercriminalidad, por ejemplo, ése fue el caso de la 41. StrÄandG, del 7 de agosto de 2007, que introdujo los §§ 202a, 202b, 202c y 303b en el CP alemán, como la ley 109/2009, denominada "Ley del Cibercrimen", adoptada el 15 de septiembre de ese año por Portugal […] Posteriormente, la decisión marco 2013/40/EU, dictada el 12 de agosto de 2013 por el Parlamento Europeo y Consejo de la Unión Europea, bajo los términos del art. 83 del Tratado de Lisboa, ha venido a complementar la citada decisión2005/222/JI con el objetivo de extender el campo de acción de la política criminal orientada a la tutela de la integridad de los sistemas informáticos […] En consecuencia, este instrumento internacional establece la necesidad de sancionar aquellas conductas vinculadas con el acceso no autorizado a los sistemas informáticos (art. 3), el ataque contra su integridad (art. 4), la destrucción de datos (art. 5) y su interceptación (art. 6). También se pone el foco de análisis sobre las herramientas informáticas (software) utilizadas para la comisión de esos comportamientos lesivos, en especial, se recomienda la punición de la conducta de creación, venta, puesta a disposición de esos programas maliciosos mediante su introducción, distribución o de cualquier otro modo, con la finalidad de la comisión de algunas de las conductas descriptas en los arts. 3 a 6 de este documento. Los objetos abarcados son programas maliciosos, códigos de seguridad o acceso que permitan el ingreso no autorizado a la totalidad, o sólo una parte, de un sistema informático…"

[188] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características.* En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 59.

información como bien jurídico protegido dentro del esquema penal; por medio de dicha ley se modificó el CP de ese país, se creó un nuevo bien jurídico denominado: *"de la protección de la información y de los datos";* y el capítulo se tituló: *"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos."*[189] Dentro de esa misma línea de análisis, recurriendo a un instrumento jurídico internacional, el Convenio de Cibercrimen de Budapest, en el Capítulo II, sobre medidas que deben adoptar los Estados a nivel nacional, en la Sección 1 - *"Derecho penal sustantivo"*, el Título 1 se denomina *"Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"*. De acuerdo con lo anterior, siguiendo una interpretación literal del numeral 217 bis del CP, no se puede afirmar que la información o la autodeterminación informativa, están excluidos como bienes jurídicos tutelados de la norma en estudio.

Inclusive el mismo autor Ulrich Beck señaló en 1986: *"…En la medida en que la unidad local se fragmenta y se estratifica, la información se convierte en el medio central que posibilita la relación y el mantenimiento de la unidad productiva. Con ello se hace central la cuestión acerca de quién, cómo y con qué medios detenta informaciones, y sobre quién, sobre qué y para qué. No es difícil adivinar que en las confrontaciones empresariales del futuro esas luchas por el poder de distribución y denegación de flujos de información serán una fuente importante de conflictos…"*[190] Es decir, la profecía del autor se materializó, en el sentido de que en la actualidad, la información se ha convertido en la herramienta fundamental para el mercado, la economía, la sociedad, la vida privada de las personas y otras. Entonces tomando en cuenta que la información se ha convertido en algo sensible con mucha más razón se le debe tutelar como bien jurídico que es.

---

[189] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características.* En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 59.

[190] BECK, Ulrich. *La sociedad del riesgo*. Traducción de M. ª Rosa Borrás y otros. Editorial Paidós, Barcelona, 1ª ed. 2019, p. 383.

Considera el autor Temperini que una característica de los delitos informáticos es su carácter pluriofensivo, agrega: *"...una estafa electrónica puede afectar la confidencialidad de la información, su integridad y el patrimonio (en función del sistema atacado) y puede abarcar también delitos que ataquen el orden económico y financiero..."*[191] Además, haciendo eco de Macarena López y Claudio Magliona (autora y autor de Chile), indica que las nuevas tecnologías facilitan *"nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos que de ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa*"[192]. Concluye el autor Temperini que, no cualquier información debe ser tutelada (principio derecho penal como *ultima ratio)*, y a su criterio, la confidencialidad, la integridad y la disponibilidad de la información, sí merecen un valor jurídico importante, y como ejemplo, en el supuesto de acceso indebido a un sistema informático, la lesión recae en el bien jurídico de la confidencialidad de la información.[193]

No queda duda que, la estafa informática tipificada en Costa Rica, es un tipo penal abierto. El profesor Castillo considera que en abstracto, de conformidad con el tipo penal, es posible una tercera modalidad de comisión de la estafa informática, a parte del uso de datos falsos o incompletos, y del uso indebido de datos, la cual es *"…valerse de alguna operación informática o artificio tecnológico, o bien, por cualquiera otra acción que incida en el procesamiento de datos del*

---

[191] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características.* En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p 59.

[192] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características.* En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 60.

[193] TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características.* En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 60.

sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual produce u obtenga un beneficio patrimonial (o) indebido para sí o para otro". En ese sentido refiere que, tal modalidad es básicamente una previsión que realizaron las personas que legislan, vislumbrando que a futuro puedan existir nuevas técnicas de manipulación informática[194]. Debido a ello no será motivo de análisis en la presente investigación esa forma de comisión, pero si vale aclarar que la última frase del primer párrafo del artículo, es aplicable para las tres modalidades de comisión, y expresamente indica que quien realice la acción debe hacerlo con la finalidad de que: *"…procure y obtenga un beneficio patrimonial o indebido para sí o para otro…"*

En este punto, toma especial trascendencia la actividad de pesca de información, en la cual según el profesor Castillo, el hecho de obtener fraudulentamente, mediante correo electrónico (engaño), los datos (códigos secretos bancarios) de la víctima, no implica *per se*, la causación de un perjuicio patrimonial ni peligro para él, siendo necesario el uso de esos datos en el sistema automatizado de información para subsumir la conducta en el 217 bis del CP.[195] Considero que el autor lleva razón, ya que, el hecho de obtener los datos mediante engaño, implica necesariamente que el autor incurrió en actos preparatorios, pero no de una estafa general, sino eventualmente de una estafa informática. Recordemos que, para la configuración de la estafa informática, es irrelevante la forma en que el sujeto activo obtuvo los datos que usará *a posteriori.* Si bien es cierto, el sujeto activo engaña a la víctima para obtener la clave de acceso, ese suministro de información, no puede considerarse como una disposición patrimonial, descartándose por ende una autolesión patrimonial, por lo tanto, no nos encontramos ante una estafa general. Si se llegara a considerar que suministrar información o datos, implica una disposición patrimonial, sería incurrir en una analogía *in malam partem*, a la cual se recurriría para reprimir y sancionar

---

[194] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 105.

[195] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 136.

conductas, lo cual se encuentra proscrito en nuestro ordenamiento jurídico, propiamente en el artículo 2 del CPP[196], y es una vulneración al principio de *lex stricta* o máxima taxatividad legal[197]; tampoco sería correcto recurrir a una argumentación evolutiva[198] del tipo penal, puesto que de hacerlo se estaría incurriendo en una vulneración flagrante al principio de estricta legalidad que rige nuestra materia penal.

Ahora bien, si el agente desiste voluntariamente de obtener el beneficio patrimonial, es decir, no usa en un sistema automatizado esos datos que fueron obtenidos previamente de forma fraudulenta, se descartaría el delito de estafa informática, puesto que no se llevaron a cabo todos los actos de ejecución para su

---

[196] Ver en contrario lo indicado por el jurista nacional Manuel Rojas Salas, quien refiere en relación con el delito de estafa general: *"Si se trata de situaciones en donde el sujeto se desprende de la cosa o de la porción del patrimonio y la entrega en el mismo acto al sujeto activo, que es quien entra en posesión y disposición en ese mismo momento, se podrá señalar que se configura a plenitud el binomio perjuicio-provecho. Pero podría acontecer que el sujeto pasivo disponga la emisión de un título-valor por ejemplo y que el sujeto activo o el tercero, no lo ponga a circular, ni lo haga efectivo durante un tiempo. En este supuesto, es evidente que la lesión patrimonial se habrá producido desde el momento de la pérdida de disponibilidad, con independencia de que el sujeto activo no haya obtenido ese propósito motivante de su actuación. Lo mismo sucede en otras latitudes, como por ejemplo en España, en donde se exige el ánimo de lucro, y es factible que a pesar de haberse concretado la lesión patrimonial, el agente activo no haya logrado el lucro propuesto inicialmente. Se aprecia entonces que la obtención del beneficio económico por parte del sujeto, puede acontecer o bien, no tener lugar. En todo caso, si se ha dado el resultado, en el tanto el acaecimiento del perjuicio, el hecho se tendrá como consumado y el beneficio que pueda obtenerse vendrá a ser un mero acto de agotamiento, que no tiene relevancia para los efectos de la consumación, sino únicamente para eventual fijación de la penalidad."* ROJAS SALAS, Manuel. *El concepto de perjuicio patrimonial en tipos penales que protegen el patrimonio*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 572.

[197] Ver CALDERÓN CHINCHILLA, Rosaura. *El principio de legalidad ¿muro de contención o límite difuso para la interpretación de la teoría del delito en C.R.?* Editorial Investigaciones Jurídicas S.A., 2ª ed. San José, 2018, pp. 30-34.

[198] Ver en ese sentido GARCÍA FIGUEROA, Alfonso; GASCÓN ABELLÁN, Marina; MARCILLA CÓRDOBA, Gema; PRIETO SANCHÍS, LUIS. *Argumentación jurídica*. Tirant lo Blanch. Valencia. 2014, p. 261: "*Argumento evolutivo o actualizador: está muy vinculado al argumento teleológico y establece que la interpretación de los textos normativos —especialmente de los que se crearon hace mucho tiempo— debe cambiar cuando cambien las circunstancias (económicas, sociales, culturales, etc.) en las que deben ser aplicados. Se trata, por tanto, de adaptar leyes viejas (o relativamente viejas) a situaciones nuevas que no pudieron ser previstas por el legislador histórico; y se basa en la asunción de que aunque los textos legales permanezcan inmutables, la voluntad de la ley o la ratio legis (cualquier cosa que esto sea) exige adaptarla a las nuevas circunstancias. La interpretación evolutiva se opone, pues, a la interpretación originalista, más vinculada a la voluntad del legislador."*

consumación. Sin embargo, el agente sería responsable de los delitos de pasaje en los que incurrió al momento de obtener mediante engaño esa información privada de la víctima, en tanto pareciera que, aunque obtuvo los datos fraudulentamente valiéndose de una operación informática, y que inclusive ya los almacenó, todavía no los ha usado en un sistema automatizado de información, *ergo*, no ha incurrido en todos los elementos objetivos del tipo penal de estafa informática. A pesar de lo anterior, como delito de pasaje, no se debe dejar de lado la posible comisión del delito de *"violación de datos personales"*, del artículo 196 bis del CP.

Asimismo, en el supuesto que el sujeto activo, una vez obtenidos los datos de la víctima mediante engaño, los use en un sistema automatizado de datos, obteniendo un beneficio patrimonial para sí, nos encontraríamos ante la estafa informática y no la estafa general. Nótese que ni siquiera nos encontramos ante un concurso aparente de normas, ya que no se cumplen los elementos objetivos del tipo penal 216 del CP. El profesor Castillo señala: *"Los intereses del derecho-habiente de datos y del propietario de cosas corporales son similares: ambos tienen un interés legítimo, que la sociedad respeta, que les permite excluir a cualquiera sin derecho a gozar de ellos e impedir daños y retiros de la cosa o del derecho. Ambos gozan de una protección absoluta, es decir, frente a cualquiera."*[199] A mi criterio, es posible deslindar el daño patrimonial del suministro de la información bancaria mediante engaño.

No está demás indicar que, cuando un supuesto fáctico pueda ser subsumido tanto en el delito de estafa general como en el de estafa informática, la primera de ellas, prevista en el artículo 216 del CP, desplaza a la segunda, estipulada en el artículo 217 bis del mismo cuerpo normativo, toda vez que ésta última (estafa informática) es subsidiaria a la primera (estafa general).

---

[199] CASTILLO GONZÁLEZ, Francisco. *La estafa informática de "Lege lata" y de "lege ferenda"*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 286.

No se omite hacer referencia en el presente capítulo, que el artículo 217 bis del CP, segundo párrafo, contiene una agravante, la cual se presenta "…*si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos…"* Pero en realidad, esa descripción no establece ningún verbo, es decir, se constituye en un agravante para los comportamientos humanos que fueron descritos en el primer párrafo del citado numeral.

De conformidad con lo anterior, se puede considerar que la estafa informática en Costa Rica, no es un tipo penal que tutela únicamente el bien jurídico del patrimonio, toda vez que, para su consumación, se ven comprometidos sistemas informáticos, así como información de distinta índole, lo cual es insoslayable. Y es en ese sentido que, el bien jurídico de la autodeterminación informativa entra en escena, siendo un pilar fundamental, toda vez que, en cierta forma de comisión, de no darse lesión a la autodeterminación informativa (por ejemplo, con el uso debido de datos), no podría configurarse el delito de estafa informática.

Derecho comparado

Si bien, en el desarrollo de la investigación, hemos aludido a otras legislaciones, de seguido, se hará una referencia superficial, a cómo se tipifica la estafa informática en otras latitudes:

Alemania

En el artículo §263a del CP alemán se sanciona el delito de estafa informática[200] de la siguiente manera: *"(1) Quien, con el propósito de obtener una*

[200] Traducido por BALMACEDA HOYOS, Gustavo. *El delito de estafa informática en el derecho europeo continental*. En: Revista de Derecho y Ciencias Penales, Nº 17, Chile, 2011, p. 114. Versión electrónica en: https://dialnet.unirioja.es/descarga/articulo/4200389.pdf.

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".

El profesor Castillo González señala que, efectivamente el bien jurídico tutelado por el parágrafo 263 a StGB, es el patrimonio de manera principal, pero de manera inmediata también se protege el interés general referente al funcionamiento del sistema de computadores tanto en la economía como en la administración.[201]

Un elemento que encuentra identidad con el costarricense, es que se sanciona el uso indebido de datos, en ese sentido, el profesor Castillo, señala: *"El art. 217 bis Cód. pen., como el §263a del Código Penal alemán, considera las intervenciones no autorizadas por el derecho-habiente en los datos, informaciones o programas, que influyen en el sistema de procesamiento de datos en funcionamiento y que tienen como resultado final la traslación de un valor de un patrimonio a otro, como una modalidad de acción."*[202] También, de modo similar al nuestro, *"el legislador alemán estableció en el § 263 a StGB como última modalidad de acción la conducta punible consistente en producir un efecto no autorizado en el funcionamiento del sistema automatizado de datos. La idea*

[201] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 69.

[202] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 85.

perseguida por el legislador alemán fue la necesidad de prever futuras formas de influir en el sistema de procesamiento de datos hoy día desconocidas."[203]

Un tema realmente relacionado con el uso de tarjetas bancarias en el Derecho alemán, es el que se refleja en el siguiente extracto: ***"La sustracción de una tarjeta codificada por parte del hermano del titular y su uso no autorizado en un cajero automático cuyo resultado fue la extracción de dinero de la cuenta del usuario brindó la oportunidad para discutir el sentido y alcance de esta conducta. Las posiciones de la jurisprudencia pasaban por rechazar la configuración del delito de hurto, ya que el autor no había tenido intención de apoderamiento de la cosa mueble, sino tan sólo la finalidad de uso (furtum usus). A su vez, el suministro de dinero por parte del cajero automático tampoco representaba el quiebre del ámbito personal de guarda de la víctima. La máquina entrega el dinero y no existe en este caso una invasión del dominio del autor, es decir, no hay sustracción. Las dificultades apuntadas para la correcta subsunción de esta conducta en el delito de hurto o de estafa informática compelió a los autores de este trabajo a solicitar la incorporación de un tipo penal especial que abarcase estos casos. Esta situación fue finalmente regulada en el § 263a del Código Penal alemán mediante la ley de reforma del 22 de noviembre de 2003"***.[204]

De esa manera el § 263a del CP alemán fue modificado en el año 2003, siendo que extendió el ámbito de aplicación a conductas meramente preparatorias de tenencia, suministro y distribución de programas maliciosos. En resumen dicha figura delictiva, reprime cuadro modalidades distintas de fraude informático.[205]

---

[203] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, pp. 106 y 107.

[204] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 305. El resaltado no corresponde al original.

[205] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 344.

Argentina

En la República Argentina, el delito de fraude informático se tipifica en el inciso 16) del artículo 173 del CP, sancionado con una pena de 1 mes a 6 años de prisión, de la siguiente manera: *"El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos"*. Nótese que, no se contempla el uso indebido de datos, además, el tipo penal es de resultado, por lo tanto, admite la tentativa. Indica el autor Gustavo Aboso, partiendo del concepto de manipulación en sentido estricto que, la *"acción de manipular debe producir una alteración en el sistema de almacenamiento y tratamiento de datos. Esta alteración debe consistir en el funcionamiento anómalo del sistema"*[206]. Por su parte, el numeral 172 del CP argentino, establece la estafa clásica de la siguiente manera: *"Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño"*.

A la luz de ambos tipos penales (172 y 173), la autora Matilde S. Matínez señala que: *"El clásico delito de estafa, tal y como está regulado por el art. 172 del Código Penal autóctono, no logra abarcar los casos donde no existe ninguna persona que actúa erróneamente a partir del ardid desplegado por el autor […] En los casos de fraude informático, es necesario descartar el error de la víctima llevado a cabo por el ardid o engaño del autor, pues este manipula una máquina con el objeto de obtener un beneficio económico en perjuicio patrimonial del afectado..."*[207] Con la promulgación de la ley N.º 26388, en el año 2008,

---

[206] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 319.

[207] S. MARTÍNEZ, Matilde. *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, pp. 38 y 39.

denominada *"Ley de Delitos Informáticos"*[208], se adicionó al artículo 173 del CP argentino el inciso 16), consecuentemente, considera la autora, se puede prescindir de la *"secuencia "ardid-error-perjuicio económico"*, toda vez que el espectro de subsunción de las conductas se amplió para los fraudes y estafas informáticas.[209]

Por su parte, el autor Gustavo Aboso, señala que la ley 25.390 (2004) introdujo el párrafo 15 al artículo 173 del CP argentino, para reprimir el uso fraudulento de una tarjeta de compra, crédito o débito: *"El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática."* Considera el autor que el bien jurídico es el patrimonio.[210] Para dicho jurista, se configura ese delito cuando el agente emplea la tarjeta en un cajero electrónico, ya sea para obtener dinero, realizar transferencias dinerarias, o hace pago electrónico de servicios o adquiere bienes.[211]

En cuanto a la información pescada –*phishing*-, y a la luz del derecho penal argentino, se ha indicado: *"debemos alertar que esta modalidad de fraude electrónico debe estar precedida de una manipulación del sistema informático, ya que acá no existe la relación de causalidad engaño-error-disposición patrimonial*

---

[208] S. MARTÍNEZ, Matilde. *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 36.

[209] S. MARTÍNEZ, Matilde. *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, p. 39.

[210] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 303.

[211] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 307.

viciada-perjuicio. En consecuencia, si la conducta del autor consistió en mantener una conversación telefónica o mediante cualquier otra vía y así logró que la víctima le haya proporcionado los datos de acceso al sistema, no encuadra en esta figura de fraude del inc. 16 del art. 173 del Código Penal argentino. En ese caso, podrá aplicarse la figura prevista por el inc. 15 de ese mismo artículo, que regula como modalidad de fraude el uso indebido de datos a través de una operación automática. El engaño utilizado por el autor, al invocar la calidad de representante de la entidad bancaria, puede ser juzgado como un engaño suficiente para provocar el error ajeno […] ***El thema decidendum en este caso es determinar si la entrega bajo error de la víctima de sus datos de acceso al sistema bancario representa ya una disposición patrimonial****…"*[212]

Asimismo, en cuanto a subsumir conductas de uso de tarjetas en el delito de hurto, se señala: *"Por último, resulta conveniente matizar este tema de la tutela del patrimonio en el ámbito de la cibercriminalidad al señalar que nuestro Código Penal no equipara, en el caso de la figura agravada de hurto del art. 163, el uso de tarjetas magnéticas o perforadas para acceder al lugar donde se encuentra depositada o guardada la cosa mueble ajena. En cambio, la legislación penal española ha previsto esta equiparación en el art. 239, inc. 3°, in fine, razón por la cual el uso de ese tipo de instrumentos para abrir dispositivos mecánicos o electrónicos califica como robo con fuerza en las cosas."* [213]

España

El CP de España establece en el artículo 248: *"1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. 2.*

[212] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 331. El resaltado no corresponde al original.

[213] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 298.

También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero."[214] Para quienes incurran en dichas conductas se prevé en el numeral 249, lo siguiente: *"Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción. Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses."* Señala la autora Salinero Alonso: *"Los supuestos en los que el agente se sirve de medios informáticos para cometer el engaño –utilización de una página web- se ventilarán por el artículo 248.1 CP y no por el artículo 248.2.a) CP."*[215]

Propiamente la estafa informática se regula en el inciso 2.a del artículo 248 del Código de España[216], nótese que el verbo activo es amplio ya que indica que el sujeto activo debe incurrir en una manipulación o artificio informático, dicha modalidad de comisión fue adoptada desde el año 1995. Considera además el

---

[214] El subrayado no corresponde al original.

[215] SALINERO ALONSO, Carmen. *Delitos contra el patrimonio (III). Defraudaciones: Estafa. Apropiación indebida. Defraudaciones de fluido eléctrico y análogas*. En: Lecciones de derecho penal: delitos contra la vida, las personas y el patrimonio, parte especial. Tomo III. Editorial Jurídica Continental, 2ª ed. San José, 2017, p. 511.

[216] *"Sin embargo, al no darse el engaño y el error, falta la esencia de la estafa. Por ello, el legislador se refiere a ella con la consideración de estafa en un apartado distinto."* SALINERO ALONSO, Carmen. *Delitos contra el patrimonio (III). Defraudaciones: Estafa. Apropiación indebida. Defraudaciones de fluido eléctrico y análogas*. En: Lecciones de derecho penal: delitos contra la vida, las personas y el patrimonio, parte especial. Tomo III. Editorial Jurídica Continental, 2ª ed. San José, 2017, p. 510.

autor Gustavo Aboso: *"…el art. 248.2.a del Código Penal español regula el fraude informático en un sentido similar, recurriendo a la técnica legislativa de equivalencia con la figura de estafa, sustituyendo en esta empresa los elementos configuradores de la estafa (engaño-error-desplazamiento patrimonial perjudicial) por la manipulación de datos, programas y sistemas informáticos, la transferencia indebida de fondos y el perjuicio patrimonial."*[217]

El mismo autor Gustavo Eduardo Aboso, remitiéndose a Muñoz Conde, señala que el art. 239, inc. 3°, *in fine*, del CP español[218], equipara el uso de llaves falsas a las *"tarjetas magnéticas o perforadas, los mandos o instrumentos de apertura a distancia y cualquier otro instrumento tecnológico o eficacia similar"*. En consecuencia, esa conducta debe ser calificada como robo con fuerza y no como hurto."[219]

El *supra* citado jurista agrega que, el fraude mediante utilización de tarjeta de crédito clonada o copiada, ha sido regulado en el art. 399 bis del CP español[220], a partir de la LO 5/2010.[221] Resulta similar lo previsto en el artículo

---

[217] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 321.

[218] Art. 239, inc. 3°, *in fine*, del CP español *"Se considerarán llaves falsas: 1. Las ganzúas u otros instrumentos análogos. 2. Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal. 3. Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.* ***A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, los mandos o instrumentos de apertura a distancia y cualquier otro instrumento tecnológico de eficacia similar****."* El resaltado no corresponde al original.

[219] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 303. El numeral 238 del CP español indica: *"Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes: 1. Escalamiento. 2. Rompimiento de pared, techo o suelo, o fractura de puerta o ventana. 3. Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.4. Uso de llaves falsas. 5. Inutilización de sistemas específicos de alarma o guarda."* (el subrayado no corresponde al original).

[220] El artículo 399 bis del CP español establece: *"1. El que altere, copie, reproduzca o de cualquier otro modo falsifique tarjetas de crédito o débito o cheques de viaje, será castigado con la pena de prisión de cuatro a ocho años. Se impondrá la pena en su mitad superior cuando los efectos*

248.2.c) del Código de España, cuando indica: *"Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes*[222] *en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero"*; con lo previsto en el numeral 399 bis. 3 de ese mismo Código, cuando sanciona a *"…El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados será castigado con la pena de prisión de dos a cinco años."* La distinción radica en cuanto a que, el 248.2.c) no hace referencia a una falsedad del instrumento, mientras tanto, en el 399 bis. 3, sí contempla ese elemento objetivo.

Nótese que ambos tipos penales prevén un perjuicio patrimonial, por lo tanto, no resulta del todo correcto el siguiente comentario que trata de identificar el elemento diferenciador entre dichos tipos penales, el cual refiere que el artículo 399 bis. 3 *"…exige la coincidencia de tres elementos: a) El uso de la tarjeta falsa, en cualquier sitio que admitan su utilización como medio de pago. b) Un elemento subjetivo, caracterizado por el conocimiento de su falsedad. c) El uso debe hacerse en perjuicio de tercero, lo que supone un menoscabo de tipo patrimonial*

---

falsificados afecten a una generalidad de personas o cuando los hechos se cometan en el marco de una organización criminal dedicada a estas actividades. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los anteriores delitos, se le impondrá la pena de multa de dos a cinco años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33. 2. La tenencia de tarjetas de crédito o débito o cheques de viaje falsificados destinados a la distribución o tráfico será castigada con la pena señalada a la falsificación. 3. El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados será castigado con la pena de prisión de dos a cinco años." (el subrayado no corresponde al original).

[221] ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017, p. 314.

[222] *"Los datos obrantes en los instrumentos de pago que tipifica el precepto comprende cualquier tipo de información que permita operar con cargo a la tarjeta, no solo los más conocidos como son el nombre y apellidos del titular, la numeración de las tarjetas, la fecha de caducidad, el n.° de seguridad –el denominado n.° CCV-, sino también, el n.° de identificación personal –PIN- o el asistente virtual VINI."* SALINERO ALONSO, Carmen. *Delitos contra el patrimonio (III). Defraudaciones: Estafa. Apropiación indebida. Defraudaciones de fluido eléctrico y análogas*. En: Lecciones de derecho penal: delitos contra la vida, las personas y el patrimonio, parte especial. Tomo III. Editorial Jurídica Continental, 2ª ed. San José, 2017, p. 513.

para el titular de documento falseado o para la entidad que lo emite o a la que se le carga el montante económico producto de la operación realizada por el autor de la acción. Precisamente este último elemento es el que introduce un elemento diferenciador en el ámbito de aplicación de esta norma para distinguirla del supuesto de estafa con uso de tarjetas o cheques de viaje, introducido por LO 5/2010, en el artículo 248.2.c)…"[223]

Resulta importante visibilizar que, las penas previstas en esos países para la estafa informática, no sobrepasan los márgenes estipulados por el legislador costarricense, el cual oscila en el numeral 217 bis del CP entre los 3 y 10 años de prisión. Mientras tanto en Alemania en el artículo §263a del CP alemán, se sanciona con pena de prisión de *"hasta cinco años o con multa"*. En Argentina el artículo 173 del CP, prevé una pena tanto para el fraude informático como para el uso indebido de datos de 1 mes a 6 años de prisión; y en España, artículo 248 del CP, dispone en abstracto la pena de prisión de 6 meses a 3 años.

Otro aspecto que llama la atención, es que ni España ni Argentina, incorporan el verbo "influir" en el tipo penal de fraude o estafa informática, simplemente hacen referencia a "*manipulación informática o artificio semejante"* y a "*manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos"*; mientras tanto en Alemania, no se contempla el verbo "manipular", pero sí "influir": "*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"*. En ese sentido, recordemos que el 217 bis del CP costarricense, incluye los verbos "influir" y "manipular", generando una confusión importante al momento de aplicar el derecho para el operador jurídico.

---

[223] GONZÁLEZ AGUDELO, Gloria. *Falsedades*. En: Lecciones de derecho penal: Delitos contra la colectividad, las administraciones públicas y los valores constitucionales. Tomo IV. Editorial Jurídica Continental, 2ª ed. San José, 2017, p.p 186 y 187. El subrayado no pertenece al original.

Capítulo III. Fundamentos legislativos para la construcción del tipo penal de estafa informática

Resulta nuclear en esta investigación, develar los argumentos de la y el legislador costarricense, al momento de construir el artículo 217 bis del CP.

Antes de ello, es importante recordar que la introducción de la informática en el derecho, no es tarea sencilla, por lo tanto, se requiere de personas capacitadas para construir derecho informático, el cual ha sido definido como *"el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en la que exista algún bien que es o deba ser tutelado jurídicamente por las propias normas" (Carpizo & Carbonell, 2003: 193)."*[224] Para los autores Béhar Quiñones y Yáñez Figueroa, aun y cuando, esa definición auxilia en el entendimiento de la materia a regular, *"**recae en el desafortunado problema de pretender regularlo desde los sistemas jurídicos tradicionales, lo que conlleva serios problemas, dadas las características que forman parte del mundo cibernético. Esto es una constante en el mundo jurídico: la mayoría de las definiciones que se han creado en torno a la informática tiende a seguir en similares condiciones a la definición expuesta y, por tanto, dejan de lado el amplio espectro que la realidad virtual conlleva. Es importante comprender que el mundo virtual tiene sus propias reglas, sus propios espacios de existencia completamente fuera de la realidad material, presencial y temporal**..."*[225] Dichos autores, evidencian de una manera muy clara esa problemática a la que se enfrentan quienes legislan con el siguiente ejemplo: *"imagine un programa de cómputo creado en Río de Janeiro, Brasil, que se encuentra hospedado en servidores de computadoras ubicados en instalaciones secretas y subterráneas en la provincia de Alberta, Canadá. El programa es utilizado por usuarios en 19 naciones*

[224] BÉHAR QUIÑONES, Gastón y YÁÑEZ FIGUEROA, Agustín. *Introducción a los contratos tecnológicos*. Editorial Tecnológica de Costa Rica, 1ª ed. Cartago, 2017, p. 17.

[225] BÉHAR QUIÑONES, Gastón y YÁÑEZ FIGUEROA, Agustín. *Introducción a los contratos tecnológicos*. Editorial Tecnológica de Costa Rica, 1ª ed. Cartago, 2017, p. 17. El resaltado no corresponde al original.

diferentes y utiliza "espejos" que respaldan la información contenida en sus bases de datos por medio de satélites que reenvían automáticamente la información cada hora a otros servidores en Japón y México. Sin necesidad de especificar las funciones de este programa, del ejemplo anterior se puede observar lo complejo que resulta para un sistema jurídico tradicional crear parámetros de regulación para algo que viaja por el mundo, que se copia y al que se accede desde muy diversos puntos."[226]

Las características propias que tiene el ciberespacio que dificultan la labor legislativa, entre otras tenemos las siguientes[227]:

- El ciberespacio no es algo material, es virtual.
- El ciberespacio, debido a su virtualidad, escapa en todo momento a las posibilidades de control efectivo de los Estados por medio de regulaciones.
- El espectro de acción dentro del ciberespacio es tan amplio y dinámico que cualquier control y regulación pueden ser evadidos con facilidad o, en su caso, resultan insuficientes para dimensionarlo.
- Entre quienes redactan las leyes y los operadores del derecho existe un desconocimiento generalizado sobre el funcionamiento técnico del mundo virtual.
- Si no se puede garantizar que toda la información se encuentre dentro de plataformas seguras en la red, cerradas y de difícil acceso, se pueden generar problemas y peligros en el mundo real.

Ahora bien, expuesto ese panorama, debemos mencionar que el delito de estafa informática del numeral 217 bis del CP, se conoció en la Asamblea Legislativa mediante el proyecto de ley tramitado bajo el expediente N.º 17.613,

---

[226] BÉHAR QUIÑONES, Gastón y YÁÑEZ FIGUEROA, Agustín. *Introducción a los contratos tecnológicos*. Editorial Tecnológica de Costa Rica, 1ª ed. Cartago, 2017, p. 17.

[227] Tomadas de BÉHAR QUIÑONES, Gastón y YÁÑEZ FIGUEROA, Agustín. *Introducción a los contratos tecnológicos*. Editorial Tecnológica de Costa Rica, 1ª ed. Cartago, 2017, p. 20.

denominado finalmente como: *"Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal"*. En un inicio el proyecto fue denominado: *"Reforma al artículo 229 BIS del Código Penal y adición de un nuevo capítulo denominado "Delitos Informáticos",* fue impulsado por el diputado Luis Antonio Barrantes Castro del partido político Movimiento Libertario.

Dicho expediente legislativo, en fecha 06 de noviembre de 2012, se convirtió en Ley de la República N.º 9048, mediante la cual se incluyó en el ordenamiento jurídico el tipo penal analizado. Es importante mencionar que, para el momento en que se discutió el proyecto, Costa Rica no era parte del Convenio sobre Ciberdelincuencia desarrollado en Budapest el 23 de noviembre de 2001[228] (con entrada en vigencia el 01 de julio de 2004), fue hasta el 18 de mayo de 2017, que se aprobó en segundo debate en la Asamblea Legislativa el expediente N° 18.484, consistente en la adhesión de Costa Rica al citado convenio[229], lo cual desembocó en la promulgación de la Ley N° 9452 del 26 de mayo de 2017, publicada en el Alcance N° 171 de La Gaceta Digital N° 125 del 03 de julio de 2017, con entrada en vigencia el 01 de enero de 2018.

Tal y como lo dijimos y a modo de antecedente, previo a la promulgación de la ley N.º 9048, el numeral 217 bis del CP contenía el delito de fraude informático, que rezaba de la siguiente manera: *"**Fraude informático.** Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que*

---

[228] Asamblea Legislativa. Expediente N° 17.613 *"Reforma a varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, y al Título VII del Código Penal"*. Oficio del Ministerio de Relaciones Exteriores y Culto, N.º DM-DGPE/576-11 del 09-11-2011, p. 975.

[229] Ver NEXOS, 2017. *Aprobado convenio sobre ciberdelincuencia*. En: https://www.nexos.co.cr/contenido/legislacion/plenario/; y PRESIDENCIA DE LA REPÚBLICA DE COSTA RICA, 2017. *Costa Rica se adhiere a Convenio contra Ciberdelincuencia*. En: https://presidencia.go.cr/comunicados/2017/05/costa-rica-se-adhiere-a-convenio-contra-ciberdelincuencia/.

incida en el proceso de los datos del sistema." (Así adicionado por el artículo 1° de la Ley N° 8148 de 24 de octubre del 2001). Dicho numeral fue reformado por la actual redacción de la estafa informática.

Vale referir en primer lugar que, mediante lo que se puede considerar como una técnica legislativa inadecuada, se mantuvo el número del artículo 217 del CP con la denominación "bis", forma que ha sido cuestionada, tal y como lo refirió la jurista nacional Rosaura Chinchilla Calderón: *"...el uso de las fórmulas legislativas "bis, ter, quáter" es inapropiado porque los cuerpos normativos son sistemas que tienen referencias internas, de modo que introducir artículos así (y, peor aún, correr numeraciones), suele generar enormes distorsiones en el sistema. Por ejemplo, cuando se incorporó el delito de tortura en medio de los de lesiones, sin darse cuenta de que había un último numeral que agravaba la pena "para los tres artículos anteriores". Como en esta materia hay que interpretar restrictivamente, por rebote se agravó aún más la sanción de la tortura (algo no querido por el legislador) y se despenalizó una agravante de las lesiones gravísimas (lo que tampoco se buscaba)..."*[230]

En el caso que nos ocupa, el CP contempla el delito de estafa general en el artículo 216; el numeral inmediato siguiente es el 217 que tipifica el delito de estelionato; y continúa el artículo 217 bis que describe la estafa informática. De acuerdo con ello, podría pensarse que la estafa informática tiene como base la figura del estelionato, sin embargo, ello no es así, el vínculo es con el numeral 216 del CP[231], se desprende entonces que, no existe una armonía ni coherencia en esa seguidilla de numerales.[232]

---

[230] CALDERÓN CHINCHILLA, Rosaura. *Crímenes de odio*. Delfino. En: https://delfino.cr/2019/06/crimenes-de-odio/, 05-06-2019.

[231] Para muestra de ello, se puede observar el informe técnico jurídico del Departamento de Servicios Técnicos de la Asamblea Legislativa del proyecto de ley: *"Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*, expediente N.º 17.613., Oficio ST. 039-2010J, del 10-03-2010. p. 36., el cual dice: *"Es preciso distinguir entre el delito típico o genérico de Estafa regulado mediante el artículo 216 del Código Penal y la norma identificada como Fraude Informático regulado mediante el artículo 217 bis, norma implementada mediante Ley N.º 8148 del 24 de octubre del 2001, en realidad lo que esta norma regula es una Estafa Informática en forma específica."*

Discusión legislativa

El primer cambio esencial que realizó el legislador, fue el de nombrar el tipo penal 217 bis como "estafa informática", generando desde ese momento el paso a la discusión, en tanto consideró que a una computadora se le puede engañar, lo cual fundamentó el legislador costarricense de la siguiente manera: *"Es preciso distinguir entre el delito típico o genérico de Estafa regulado mediante el artículo 216 del Código Penal y la norma identificada como Fraude Informático regulado mediante el artículo 217 bis, norma implementada mediante Ley N° 8148 del 24 de octubre del 2001, en realidad lo que esta norma regula es una Estafa Informática en forma específica. En el primer caso – la estafa- comprende el error en que se hace incurrir a una persona, por medio del engaño para lograr un beneficio patrimonial antijurídico para sí o para un tercero, logrando lesionar el patrimonio ajeno. Mientras que en la estafa informática la acción que realiza el autor es la de alterar o manipular (engaño) el ingreso, procesamiento y salida de datos de un sistema de cómputo, por medio de programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema, del cual se pueda generar un perjuicio para un tercero."*[233]

De dicha justificación se denota:

---

[232] Similar crítica se observa en: LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 1ª ed. San José, 2011, p. 120. Si bien para ese momento estaba vigente el delito "fraude informático", es adecuado traer a colación el siguiente comentario del autor relacionado con el extinto 217 bis del Código Penal: *"La ubicación del artículo dentro del Código Penal de Costa Rica, se encuentra en la sección IV Estafas y otras defraudaciones, lo cual es correcto, ya que la modalidad del actuar del tipo penal y en si el desarrollo del delito informático encuadra en esta sección; pero su ubicación, siendo el artículo 217 Estelionato y el artículo 217 bis Fraude Informático, es confusa; el hecho de ser 217 bis implicaría una relación directa con el artículo 217, pero en este caso no, estelionato es "en general, fraude en los contratos; despojo injusto de la propiedad ajena o cualquier engaño, sin otro nombre determinado, en convenciones y actos jurídicos" (Cabanellas de Torres, 1983), mientras el concepto fraude se refiere a "en un sentido general, engaño, abuso de confianza, acto contrario a la verdad o a la rectitud" (Cabanellas de Torres, 1983)."*

[233] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE SERVICIOS TÉCNICOS. *Informe Técnico Jurídico. Proyecto de Ley: "Reforma al artículo 229 BIS del CP y adición de un nuevo capítulo denominado "Delitos Informáticos"*. Expediente N° 17.613 J. Oficio ST. 039-2010 J, 10 de marzo de 2010. pp. 19 y 20.

1) Que tal y como se dijo párrafos *supra*, existe un vínculo entre el numeral 216 (estafa) y el 217 bis (estafa informática) del CP; y no entre el 216 (estafa) y el 217 (estelionato) del mismo cuerpo normativo. Es decir, según la secuencia lógico-jurídica y la armonía que debería regir nuestro ordenamiento jurídico, la estafa informática debería ser el tipo penal inmediato siguiente a la estafa general. La ubicación de los tipos penales adoptada por las personas legisladoras, sin lugar a dudas no es la adecuada, incluso termina siendo incoherente, y dificulta la interpretación restrictiva de dichos tipos penales.

2) Que las personas legisladoras, *prima facie*, incurrieron en error dentro de sus fundamentos, al considerar que el sujeto activo cuando "altera" o "manipula", está engañando a un sistema informático. En realidad, un sistema de cómputo no puede ser engañado de ninguna manera, tal y como lo mencionamos en capítulos precedentes, en ese sentido: *"…no es posible engañar a máquinas, ni sistemas informáticos, porque: "solo el ser humano puede ser inducido a error, es un fenómeno eminentemente sicológico que hace que la víctima del engaño, indudablemente movida por el error a que ha sido inducida, voluntariamente disponga de los bienes, con perjuicio de su patrimonio o de terceros. Las máquinas no pueden ser engañadas, las máquinas no cometen errores…"*[234]

El autor José Manuel Paredes Castañón, señala como una regla de necesaria consideración, para las personas legisladoras al momento de promulgar una ley: "*Regla 89.ª: Por fin, es particularmente importante que la enunciación de las prohibiciones jurídicas (de las normas primarias, prohibitivas) sea realizada, desde el punto de vista lingüístico, de tal modo que resulten meridianamente claros los límites de la clase de las acciones que resultan prohibidas. Y ello, no sólo –que también– por razones de seguridad jurídica, sino para asegurar una*

[234] OXMAN, Nicolás. *Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"*. En: Revista de Derecho de la Pontificia Universidad Católica de Valparaíso N° 41, Valparaíso. Versión electrónica en: http://www.scielo.cl/scielo.php?pid=S0718-68512013000200007&script=sci_arttext, 2013.

eficacia y una eficiencia razonables a la prohibición. Para ello, lo deseable es que la descripción de la (clase de) acción prohibida se haga, en la medida de lo posible, recurriendo preferentemente a términos que posean una extensión susceptible de ser determinada de manera sencilla, bien mediante el recurso al uso ordinario –e inequívoco– del lenguaje, o bien remitiéndose a un significado establecido por las ciencias."[235]

Se deriva de esa explicación y de la constancia terminológica que debería imperar dentro de un mismo texto, que el uso del lenguaje es esencial para legislar, es decir, si el delito de estafa informática fue considerado en última instancia una especie de estafa, entonces, debió describir dentro de los elementos objetivos del tipo penal, necesariamente un comportamiento humano de inducir a error a otra persona, por medio de un ardid o un engaño, pero ello no fue así; lo descrito en el numeral 217 bis del CP, relata una situación completamente distinta, *ergo*, el legislador al momento de redactar el tipo penal dejó de lado el significado literal del concepto jurídico de "estafa".

Ahora bien, compartimos parcialmente el criterio externado en el informe técnico de la Asamblea Legislativa, relativo a este proyecto de ley, en el tanto se afirmó: "*Si bien el título de la norma, no es un elemento integrante del tipo penal ya que la conducta se tipifica y sanciona en el texto de la norma con independencia de su título, lo cierto es que este resulta un elemento que facilita al operador jurídico el manejo del texto normativo."*[236] No se comparte del todo, ya que a nuestro criterio, el título del artículo sí es parte integrante del tipo penal, puesto que si no fuese así, entonces sería innecesario intitular los delitos, precisamente, denominar un delito de "x" o "y" manera, facilita la comprensión del mismo para terceras personas, brinda seguridad jurídica y permitiría, en tesis de

---

[235] PAREDES CASTAÑÓN, José Manuel. *Vademécum del legislador racional (y decente): Noventa reglas para una buena praxis legislativa en materia penal.* En: Libro-Homenaje a Claus Roxin. Editorial Talleres Gráficos Iustitia, 1ª ed. Perú, 2018, p. 235.

[236] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE SERVICIOS TÉCNICOS. *Informe Técnico Jurídico. Proyecto de Ley: "Reforma al artículo 229 BIS del CP y adición de un nuevo capítulo denominado "Delitos Informáticos"*. Expediente N° 17.613 J. Oficio ST. 039-2010 J, 10 de marzo de 2010, p. 34

principio, a las personas legisladoras construir leyes en armonía con el resto del ordenamiento jurídico.

En lo que concierne a la "exposición de motivos" del expediente legislativo N° 17.613 (documento que dicho sea de paso utiliza únicamente dos fuentes de apoyo de Internet, sean las siguientes direcciones: 1) http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico y 2) www.prensalibre.cr), el para entonces diputado del partido Movimiento Libertario, Luis Antonio Barrantes Castro, señala que la importancia de promulgar la ley de delitos informáticos, es por un tema de seguridad ciudadana y hace un enfoque contemplando varios bienes jurídicos, en el que pareciera predominar el patrimonio, señalando: *"El motivo de esta situación, no solo lo es el aumento desmedido de la delincuencia sino la sofisticación de los métodos que aplican los antisociales para perjudicar tanto la integridad física y moral así como el patrimonio de los ciudadanos […] Un ejemplo de la sofisticación de estos métodos, es el aumento de los llamados delitos informáticos; según indicó el Organismo de Investigación Judicial por medio de un comunicado de prensa, al 4 de mayo de 2009 aproximadamente 25 personas habían sido estafadas por medio de delitos informáticos a través de las campañas publicitarias de los bancos estatales, en donde las víctimas revelaban sus cuentas por Internet*"[237]. De lo anterior se determina que, la ley fue promulgada atendiendo un criterio meramente alarmista y populista, en el entendido de atacar comportamientos humanos mediante el derecho penal, sin hacer un análisis profundo sobre el tema. Llama la atención la frase: *"...25 personas habían sido estafadas por medio de delitos informáticos..."*, en realidad, el hecho de que se utilice un sistema informático (si es que a eso se refirió con la frase *"por medio de delitos informáticos"*) no implica *per se,* que estemos ante un delito de esa naturaleza.

---

[237] ASAMBLEA LEGISLATIVA DE COSTA RICA. DEPARTAMENTO DE SERVICIOS PARLAMENTARIOS. *Exposición de motivos del proyecto de Ley "Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*, expediente N.º 17.613., pp. 3 y 4.

Posteriormente, el legislador transcribe en la exposición de motivos una noticia periodística del 05 de mayo de 2009, del diario Prensa Libre: *"...Dos de los métodos más usados en Costa Rica son el Phishing y el Pharming. El primero consiste en enviar un correo electrónico a la víctima, el cual proviene de un ente oficial, pero en realidad es falso, y en cuyo contenido se hace una solicitud expresa para actualizar la información confidencial perteneciente al cliente, como el nombre de usuario, contraseña, número de tarjeta y PIN entre otros, los cuales al final terminan en las computadoras de los estafadores. La segunda técnica conocida como Pharming, es cuando mediante la alteración del Servidor de DNS de un Proveedor de Servicios de Internet (Racsa, ICE), y del DNS del Sistema Operativo de la computadora de un usuario. En este caso, es posible a través de la introducción de un programa malicioso, modificar el archivo de nombre hosts para el caso del Sistema Operativo Windows. Estos programas pueden provenir de correos electrónicos, descargas por Internet o medios de almacenamiento externos como llaves USB, entre otros. Luego de acceder al vínculo referenciado en la página de Internet enviada, se ejecuta el programa malicioso, el cual modificará el archivo hosts de la computadora del usuario, sin su conocimiento, quien finalmente luego de digitar las direcciones de Internet en su navegador será redireccionado a una página de Internet fraudulenta".*[238]

Nótese que, no se hace ninguna indicación de por qué, la estafa general no es capaz de cubrir propiamente la pesca de información mediante engaño. El profesor Castillo González, al respecto hace el siguiente comentario: *"No existe estafa informática sino una estafa general, cuando el resultado del sistema automatizado de datos está sometido al examen de una persona física. Tal es el caso de "phisching"* (sic)*, en donde es la misma víctima la que, por engaño,*

[238] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE SERVICIOS PARLAMENTARIOS. *Exposición de motivos del proyecto de Ley "Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*, expediente N.º 17.613, pp. 4 y 5.

entrega al estafador el número de carta de crédito u otro datos (sic) *secreto."*[239] A nuestro criterio, la primera parte del extracto es correcta, sin embargo, discrepamos de la segunda, toda vez que, todavía no ha existido una disposición patrimonial, lo cual excluye a la estafa convencional, dicho tópico será analizado posteriormente.

Otro elemento que llama la atención es que si bien, el bien jurídico predominante en la exposición de motivos del proyecto de ley, fue el patrimonio, también se contemplaron otros, tales como: "la información" y "la protección de datos personales", en ese sentido se indica: *"Es por esto que en aras de penalizar acciones y tutelar el bien jurídico de la información y generar herramientas eficientes y eficaces para condenar delitos informáticos que afectan cada vez más el patrimonio de los costarricenses, se presenta el siguiente proyecto de ley."*[240] Es decir, sí existió un razonamiento a tutelar el patrimonio mediante la protección del bien jurídico de la información.

Dentro del expediente legislativo N.º 17.613, se cuenta con el informe técnico jurídico del proyecto de ley, confeccionado por Cristina Ramírez Chavarría, en el mismo se menciona: *"La inexistencia de una ley de delitos informáticos que sancione penalmente de manera sistematizada en un solo cuerpo normativo los múltiples "ilícitos informáticos" ha sido elemento de críticas al sistema,* ***dada la gran cantidad de crímenes que quedan impunes****."*[241] Llama la atención dicha afirmación, toda vez que no se respalda en ningún dato estadístico o fuente, es decir, la redactora considera que la cifra negra de delitos informáticos se debía en

---

[239] CASTILLO GONZÁLEZ, Francisco. *La estafa informática de "Lege lata" y de "lege ferenda"*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 294.

[240] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE SERVICIOS PARLAMENTARIOS. *Exposición de motivos del proyecto de Ley "Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*, exp. N.º 17.613., p. 6.

[241] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE SERVICIOS TÉCNICOS. Informe Técnico Jurídico del proyecto de Ley *"Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*, exp. N.º 17.613., Oficio ST. 039-2010J, 10-03-2010. p. 22. El resaltado no corresponde al original.

aquel entonces (año 2010), a la inexistencia de una ley de delitos informáticos, conclusión que para estar dotada de contenido requería algún estudio sociológico que así lo demostrara, y es que lo manifestado es una generalidad, siendo que no todos los tipos penales informáticos tienen la misma repercusión social o tratamiento. Por el momento, basta mencionar que esa fue una de las consideraciones del Departamento Técnico Jurídico de la Asamblea Legislativa[242] para lograr la aprobación del proyecto.

De la misma manera que se hizo en la *"exposición de motivos"*, el *"Informe Técnico Jurídico"* del proyecto de ley, considera a la "información" como un bien jurídico, señala que ***"es considerada como un activo más - un derecho fundamental- respecto del que se pueden ejercer prerrogativas patrimoniales*** *(por un eventual contenido económico) o* ***morales****."*[243]

---

[242] Es insoslayable mencionar lo siguiente relacionado con el informe técnico jurídico (se aclara que no se trata de un tema relacionado directamente con la estafa informática, pero sí evidencia un error grave en lo que respecta a la argumentación jurídica expuesta dentro de la Asamblea Legislativa al momento de aprobar un proyecto de ley), de la ley N.º 9048 del 10-07-2012, el cual modificó, entre otros, el numeral 229 bis del CP, antes de la reforma, tipificaba el delito denominado: *"Alteración de datos y sabotaje informático"*, y preveía dependiendo la modalidad de comisión dos rangos de penas de prisión, la primera de 1 a 4 años y la segunda de 3 a 6 años. La propuesta según el Informe Técnico era cambiarle el nombre a *"Daño informático"*, fijando un único rango de penas de 3 a 6 años de prisión. De seguido menciona el "informe técnico jurídico", respecto a la modificación del *quantum* de las penas: ***"Elevar el rango inferior de la pena a tres años de prisión tiene como efecto que el sujeto responsable del delito quedaría excluido de la posibilidad de acogerse al beneficio de "Suspensión del procedimiento a prueba" regulado mediante el artículo 25 del Código Procesal Penal en relación con los numerales 59 y 63 del Código Penal****, toda vez que ese beneficio tiene como requisito de procedencia que se trate de un delincuente primario y la pena no exceda de tres años de prisión".* Dicho razonamiento de los personeros del Departamento de Servicios Técnicos de la Asamblea Legislativo deja muchas dudas en cuanto a la credibilidad y solvencia del informe técnico; la condena de ejecución condicional de la pena prevista en el artículo 59 del CP, efectivamente se puede aplicar cuando la pena no exceda de 3 años de prisión, es decir, que la modificación propuesta y reflejada en el informe técnico (sin importar si fue así aprobada o no) no tornaba nugatoria la posibilidad de desjudicializar el proceso penal mediante el instituto procesal de la suspensión del procedimiento a prueba. (Ver Asamblea Legislativa de Costa Rica, Informe Técnico Jurídico del Departamento de Servicios Técnicos del proyecto de Ley "Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos", exp. N.º 17.613., Oficio ST. 039-2010J, del 10-03-2010. p. 34.).

[243] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE SERVICIOS TÉCNICOS. Informe Técnico Jurídico. Proyecto de Ley *"Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*, exp. N.º 17.613., Oficio ST. 039-2010J, del 10-03-2010. p. 24. El resaltado pertenece al original.

Se agrega en el Informe Jurídico que: *"existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son: •* ***Acceso no autorizado****: Uso ilegítimo de passwords y la entrada de un sistema informático sin la autorización del propietario."*[244] Se rescata ese comentario toda vez que, se incurre en un error conceptual importante al considerar que el uso indebido de datos es una acción contra los propios sistemas, cuando en realidad, dicha modalidad de comisión no implica una alteración o ataque de esa naturaleza.

De acuerdo con el informe técnico, preliminarmente, el delito de estafa informática se iba a leer de la siguiente manera: *"Se impondrá prisión de tres a doce años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya o manipule el ingreso, procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema"*.[245] Señala además que, la norma *"...tendría el efecto de derogar el artículo 217 bis del Código Penal, dado que salvo porque agrega la frase "influya o manipule el ingreso" su contenido es idéntico, a dicho artículo […] la iniciativa agrava la pena ya que la norma vigente sanciona la conducta con prisión en el rango de uno a diez años, mientras la propuesta la eleva de tres a doce años, con lo cual se reducen las posibilidades de*

[244] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE SERVICIOS TÉCNICOS. Informe Técnico Jurídico. Proyecto de Ley *"Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*, exp. N.º 17.613., Oficio ST. 039-2010J, del 10-03-2010. p. 29.

[245] Según moción N.º 14 del diputado Walter Céspedes Salazar, Acta de la Sesión Plenaria N.º 43 del 08-07-2010, pp. 284, 285, 287 y 310., se propuso sin justificación alguna que el tope máximo de pena de prisión para el delito de estafa informática, fuera de 8 años. También se propuso sin justificación alguna, cambiar la última frase de esa redacción sea: *"uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema*" por *"uso indebido de datos que incida en el proceso de los datos del sistema"*. Dicha moción fue votada y rechazada en primer debate el 20-07-2010 (ver p. 360 del proyecto de ley (se le trata como moción N.º 13).

que el responsable de esta conducta tampoco pueda acogerse al beneficio de Suspensión del procedimiento a prueba..."[246]

Al final, la reforma aprobada mediante la ley N.º 9048 del artículo 217 bis) del CP, fijó los rangos de pena de 3 a 6 años (primer párrafo) y una agravante de 5 a 10 años (segundo párrafo). Por su parte, el fraude informático de antaño, preveía una pena de 1 a 10 años de prisión. Se determina entonces que se aumentó el extremo mínimo de la pena a 3 años de prisión.

Propiamente, el día 27 de abril de 2010, la Asamblea Legislativa emitió el dictamen afirmativo de mayoría de la *"Reforma a varios artículos del Código Penal y adición de un nuevo capítulo denominado delitos informáticos"*, como justificación se hizo referencia al oficio ST. 039-2010J (informe de servicios técnicos), que en relación a Internet dijo que: *"configura un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social. Es así como junto a las incuestionables ventajas que presenta este fenómeno de la información y las comunicaciones surgen facetas negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática"*[247]*.* Continúa señalando el dictamen *que*: *"El proyecto pretende dar un marco legal a la problemática de la utilización de los medios electrónicos por parte de la delincuencia, para realizar actos delictivos. Este consta de dos artículos: el primero hace reformas al Código Penal para así incluir manifestaciones adicionales de los delitos ya tipificados y, el segundo, propone un capítulo nuevo para este código en donde se incluyan figuras delictivas nuevas […] Se busca con la propuesta, solventar la carencia de legislación que regule*

---

[246] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE SERVICIOS TÉCNICOS. Informe Técnico Jurídico. Proyecto de Ley *"Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*, expediente N.º 17.613., Oficio ST. 039-2010J, 10-03-2010. pp. 36 y 37. El subrayado no corresponde al original.

[247] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE COMISIONES. Dictamen Afirmativo de Mayoría de la *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"* (antes denominado "*Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*)., p. 217.

actos que van en perjuicio de la sociedad pero que no han sido tipificados aún como delitos..."[248] Vale mencionar que, en ese dictamen no se hace ningún comentario específico relativo a la estafa informática. Asimismo, en el documento se transcribieron palabras de Carlos Chinchilla Sandí (ex magistrado de la STCSJ), quien según dicho documento, se mostró insistente con la regulación del tema, reveló conformidad con la iniciativa de ley, y agregó que era un proyecto de primer mundo, inclusive realizó el siguiente comentario, relacionado con el tipo penal de la suplantación de identidad: *"Estos sitios o redes sociales están cargados de personas mentirosas, de personas que no se identifican como son, de personas que tienen complejos, que tienen algún tipo de situación anómala en su desarrollo y lo que hace es suplantar identidades para cometer atrocidades contras niñas..."*[249]

Posteriormente, en el acta de la sesión plenaria N.º 51, del jueves 29 de julio de 2010, como moción N.º 4, la diputada Quintana Porras, propuso que el delito de estafa informática se leyera de la siguiente manera: "*Se impondrá prisión de tres a doce años a la persona* ***que procure u obtenga*** *un beneficio patrimonial para sí o para un tercero..."*[250] Modificando la frase: *"Se impondrá prisión de tres a doce años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero..."* Dicha moción resultó rechazada, y llama la atención que cuando se discutió, el diputado Góngora Fuentes, demostrando desconocimiento del numeral 24 del CP, realizó el siguiente comentario: *"Aquí hay que apuntar que se elimina la palabra "intención", pero la inclusión de la palabra*

---

[248] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE COMISIONES. Dictamen Afirmativo de Mayoría de la *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"* (antes denominado "*Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*), del 27-04-2010., p. 217.

[249] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. DEPARTAMENTO DE COMISIONES. Dictamen Afirmativo de Mayoría de la *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"* (antes denominado "*Reforma del artículo 229 BIS del CP y adición de un nuevo capítulo denominado delitos informáticos"*)., 27-04-2010., pp. 218 y 219.

[250] Resaltado corresponde al original.

"que procure", debe también entenderse en estado de tentativa. Si los diputados están a favor o en contra de apoyar la moción para el tipo penal, contenga tanto la tentativa como la consumación material del acto antijurídico y culpable."[251]

Como moción N.º 5 del diputado Luis Fishman Zonzinski, propuso la siguiente redacción de la estafa informática: *"Se impondrá prisión de tres a seis años al que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero..."*[252] Señaló como justificación: *"Doce años nos parece una pena excesiva, la pena existente, es el homicidio. Estamos calificando igual una estafa informática con un homicidio. Nos parece exagerado, nos parece que una pena de tres a seis años, es una pena más que justificada. En cuanto a la intención de procurar un beneficio hay que recalcar que existen en el Código Penal varios delitos, que manifiestan esa intencionalidad, al igual que el Código Tributario. La intencionalidad no es una tentativa, es una cuestión probatoria, por eso se incorpora. Y se elimina la manipulación en ingreso, la propuesta también elimina la última frase, esto es importante en este tipo penal es la acción, que es "la manipulación el ingreso, procesamiento o resultados de los datos, y no el medio que se utilice, para esa manipulación. Además, se elimina la frase abierta que es "cualquier otra acción que incida en el proceso de datos". Se está restringiendo la última frase, de donde dice: "otra acción que incida en el proceso de los datos del sistema". Otra acción, es decir, es una cuestión demasiada amplia..."*[253]

En la moción N.º 10, los diputados Góngora Fuentes y Cubero Corrales propusieron que se leyera así: *"Se impondrá prisión de tres a seis años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya o manipule el ingreso, procesamiento o el resultado de los datos* ***que consten en cualquier medio electrónico****, mediante programación,*

[251] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Acta N.º 51, 29-07-2010, p. 381. Acta de la sesión ordinaria N.º 6, 10-08-2010., pp. 457 y 458.

[252] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Acta N.º 51 de 29-07-2010, p. 381 y 383.

[253] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Acta de la sesión ordinaria N.º 6, 10-08-2010., pp. 458 y 459.

empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."[254] Posteriormente, retiró la moción, indicando además, que la pena de 12 años de prisión era muy alta.[255]

Como moción número 20 del diputado Céspedes Salazar, se propuso que la estafa informática se leyera así, la cual se adelanta, fue rechazada[256]: "*Se impondrá prisión de tres a doce años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya o manipule el ingreso, procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso normal de los datos del sistema o* ***valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero. La misma pena del delito principal pero reducida hasta en un tercio a consideración del Tribunal, se impondrá a todo aquel que aun no teniendo pleno dominio del hecho, facilite los medios o de cualquier forma colabore para la obtención del beneficio ilegítimo. Igual pena se impondrá a los propietarios de los negocios comerciales en los que con o sin fines de lucro, se facilite la conexión a Internet, para la comisión de estos delitos. La pena se reducirá en dos tercios cuando el propietario de estos negocios hubiere facilitado la comisión del delito por simple omisión de los controles y mecanismos de seguridad necesarios para prevenir la comisión de estos ilícitos o posteriormente identificar y reprimir a sus autores."***[257] En esa misma moción, el diputado Céspedes refirió la creación de un

---

[254] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Acta N.º 51, 29-07-2010, pp. 381 y 383. El resaltado corresponde al original.

[255] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Acta de la sesión ordinaria N.º 6, 10-08-2010., p 461.

[256] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Acta de la sesión ordinaria N.º 6, 10-08-2010., pp.475 y 479.

[257] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Expediente proyecto de ley 17.613*: "Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, acta N.º 51, 29-07-2010, p. 386. Y en el tercer informe de mociones vía artículo 137, 10-08-2010., p. 435, el diputado Céspedes señaló como justificación de su propuesta, lo siguiente:

nuevo tipo penal denominado hurto informático: *"Se impondrá pena de prisión de dos a diez años a quien, a través de uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación informáticos para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor."*[258]

Dentro del expediente legislativo, se observa que la Dirección Jurídica del Banco Nacional, por medio del abogado Federico Salazar Ficklin y de la Directora, Marietta Herrera Cantillo, se pronunciaron respecto al proyecto de ley de delitos informáticos (incluido el delito de estafa informática, tal y como se había propuesto en la exposición de motivos), señalaron estar conformes con la creación de nuevos tipos penales, ya que ello se adecúa a la realidad nacional; al mismo tiempo hicieron la siguiente observación "...*consideramos que la falencia que presenta en este punto el proyecto de ley es que el articulado propuesto parte de un serie de conceptos jurídicos que al no estar regulados en el mismo proyecto de ley devienen en indeterminados, así por ejemplo se utilizan los siguientes conceptos que no se explican en la normativa: SOPORTE LÓGICO; VIRUS, SOFTWARE MALICIOSO; COMPONENTES LÓGICOS. En nuestro criterio los conceptos anteriormente mencionados deben estar definidos por la misma ley, pues no pueden ser dejados a criterio de los operadores del derecho su delimitación y conceptualización, ya que al hacerlo se crearía una relativización de términos que acarrearía inseguridad jurídica dentro de los usuarios del sistema*

"Algunas de estas modificaciones parten de la experiencia que han tenido los Bancos frente a diversas delincuencias que se han producido con la utilización de los medios informáticos impactando no solo en los propios bancos sino también en los clientes, y otras tienden solamente a contribuir de alguna manera con la regulación del tema, aportando algunos conceptos que harían más específica y técnica la legislación. En sentido amplio, se incluye también dentro de esta denominación todas aquellas acciones tendentes a utilizar con vehículo de comisión del ilícito los medios informáticos, aun cuando se termine lesionando bienes como la propiedad, el patrimonio y la confianza pública entre otros. Algunos de los tipos penales que aquí se incluyen permitirán a las entidades financieras reaccionar con mayor propiedad ante eventos y personas que buscan sustraer sus recursos o los de sus clientes urdiendo fraudes y ejecutando un sinnúmero de actos de este género encaminados al mismo fin." El resaltado pertenece al original.

[258] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Acta N.º 51, 29-07-2010, p. 387.

judicial..."[259] Dicha observación fue atinada en el sentido de que atendiendo el principio de legalidad era necesario precisar los conceptos, más si se tomaba en cuenta el tipo de materia, sin embargo, los legisladores y las legisladoras, tal y como se verá al momento de aprobar la ley, hicieron caso omiso a la observación del Banco Nacional.

El 20 de agosto de 2010 con aprobación el 24 de ese mismo mes y año, de manera sorpresiva, un grupo de legisladores propuso un texto sustitutivo para el proyecto N.º 17.613, tramitado bajo la moción número 48-137. En ese momento (dicho sea de paso, último día de mociones[260]) se propuso prácticamente la actual

---

[259] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Informe de la Dirección Jurídica del Banco Nacional de Costa Rica. Expediente 17.613 "*Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos".* N.º D.J.1583-2010, REF/2223-2010, 06-08-2010., p. 402.

[260] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 "*Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, acta 66, 22-08-2010., pp. 601 y 614. El diputado José María Villalta Florez-Estrada manifestó: *"...quiero explicar las razones por las cuales proponemos devolver este proyecto a comisión con un plazo. Nosotros estamos de acuerdo con que se regule el tema de los delitos informáticos, no estamos en contra per sé del proyecto, sin embargo, en la última sesión donde se conoció el último informe de mociones 137 se aprobó un texto sustitutivo en la Comisión de Seguridad Ciudadana sobre este proyecto. Cuando un texto sustitutivo se aprueba en el último días de mociones tiene el efecto de que estaría anulando, impidiendo el ejercicio del derecho de enmienda, ese texto sustitutivo introduce cambios sustanciales, incluso, modifica otros artículos del Código Penal que no se tocaban antes, y entonces, si esto lo dejamos así imposibilitaría la presentación de las mociones de reiteración y el ejercicio del derecho de enmienda de las diputadas y los diputados, eso podría generar un vicio insustancial del procedimiento, ya hay precedentes, la Sala Constitucional se pronunció, por ejemplo, en el caso de una Plena donde se hizo algo parecido, vean ustedes el voto 200314251, y, obviamente, aunque estamos de acuerdo con la idea de que se regulen los delitos informáticos, el proyecto tiene cosas que hay que revisar, queremos ver la proporcionalidad de las sanciones, queremos que no se use el tema de los delitos informáticos para meter, por ejemplo, sanciones excesivas en temas de propiedad intelectual o el uso de programas de cómputo que nada tiene que ver y, pues, solo es posible introducir algún cambio a este nuevo texto que se aprobó si el proyecto se devuelve para un nuevo dictamen y se abre la posibilidad de ejercer el derecho enmienda..."* Dicha solicitud fue acogida por el resto de legisladores, sin embargo, el expediente legislativo no fue devuelvo a la comisión, en razón de ello, el diputado Villalta Florez-Estrada, indicó: *"Pero veo que no hay interés en corregir esos errores o, por lo menos, eso es lo que parece, entonces voy a retirar la moción, porque la verdad es que tampoco a mí me interesa obstruir este proyecto y si sale con errores, pues será responsabilidad de las otras fracciones legislativas.*" En la pp. 655 y 656, el mismo diputado manifestó: *"...si ustedes ven las penas establecidas para estos delitos, repito, estamos de acuerdo con que se regule […] pero no puede ser, por ejemplo, que la pena por hacerle daño a una computadora, el delito de daños sea mucho más alta que la del delito de daños para cualquier otro bien, eso es desproporcionado, o la reforma que le meten al delito de hurto, y entonces, resulta que ahora es más alta la pena del hurto, el que se apropia de un bien ajeno sin fuerza o sin violencia sobre las cosas, que la pena del robo simple, que es el que lo hace con violencia, no puede ser […] Tenemos un problema serio aquí, porque como la inseguridad ciudadana, es cierto, está creciendo en este país […] hay una tentación de*

redacción del delito de estafa informática, pero mantenía el título de "fraude informático"[261]. Según lo manifestado por la diputada Araya Pineda, dicho texto fue realizado por la Comisión Permanente Especial de Seguridad y Narcotráfico, ya que: *"La criminalidad informática ha evolucionado, y muchos de los delitos informáticos que pueden tener efectos en Costa Rica no respetan fronteras, por lo cual la lucha contra la "ciberdelincuencia" debe ser realizada en cooperación con otros Estados, y esta nueva propuesta contó con la ayuda de expertos en la materia, con la finalidad de que la misma sea un primer paso para que Costa Rica acceda al "Convenio Europeo sobre Ciberdelincuencia", y con esto evitar que nuestro país se convierta en un paraíso para la criminalidad informática […] Se introduce la figura del fraude informático, aquí lo importante es que en este delito se manipula un sistema informático para obtener un beneficio patrimonial indebido..."*[262]

También llama la atención lo manifestado en ese sentido por la diputada Araya Pineda, quien respecto a ese texto sustitutivo mencionó: *"...a este texto sustitutivo que se está presentando esta noche acá en la sesión y es con respecto al tema de suplantación de identidad, que está establecido en la moción. Aquí queremos dejar clara la posición nuestra en este texto, es que se castigue el delito que comete una persona que se hace pasar por otra en una red social, en un sitio de internet o en cualquier otro medio electrónico o tecnológico. Con esto no se está considerando que utilizar pseudónimos o nombres de fantasías o lo que se*

---

acoger esas propuestas de la mano dura, que muchas veces son irreflexivas o responden a mentalidades autoritarias que chocan frontalmente con los principios más elementales de nuestro sistema democrático. Legislar al calor de las secciones de sucesos de los noticieros, en materia de política criminal es el peor error que puede cometer este Parlamento, pero lo estamos cometiendo porque todos los días veo yo proyectos de ley aquí que le quieren meter pena de cárcel a todo y, entonces, si todo tiene penas de cárcel altísimas, no estamos sabiendo priorizar cuáles son los delitos que realmente hay que perseguir de forma rigurosa..."

[261] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, moción N° 48 vía artículo 137., pp. 522 y 525.

[262] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Expediente 17.*613 "Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, moción 48 vía artículo 137., p. 563.

conoce en el medio como Nick name, se considera un delito, pues no trata en ningún momento de minar la libertad de expresión, ***aquí lo que se quiere penar son delitos que se cometen utilizando la personalidad de otros, utilizando su nombre para cometer estafas, hurtos o fraudes,*** *es decir,* ***queremos evitar que por estos medios informáticos las personas abusen y causen daño a otras personas****..."*[263] Se evidencian dos situaciones: **1)** Existió una confusión con respecto a la finalidad de promulgación de tipos penales, precisamente porque mediante la tipificación del delito de suplantación de identidad se pretendió prevenir los delitos de estafa, hurto o fraudes; **2)** Se utilizó el argumento del derecho penal como herramienta preventiva y disuasoria, es decir, la prevención general negativa de la pena, fin de la sanción penal no reconocido en nuestro ordenamiento jurídico de conformidad con el numeral 51 del CP, el cual contempla únicamente la prevención especial positiva como fin punitivo[264].

El diputado Luis Fishman Zonzinski, consideró que el proyecto de ley inicial N° 17.613 era deficiente en palabras de él *"era muy malo, realmente era muy malo"*. Siendo que intentaron mejorarlo mediante el reglamento y ponencia de expertos en la materia[265], lo que desembocó en el texto sustitutivo. Consideró que: *"Puede ser que haya algunas penas que son un poco fuertes, puede ser que merezca alguna revisión, yo no tendría ningún inconveniente que el proyecto fuera enviado de vuelta a la comisión […] Por supuesto que lo que estamos haciendo son parches, por supuesto no es la manera adecuada de legislar en materia penal, es decir, tenemos que hacer un planteamiento global de una política de seguridad*

---

[263] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Expediente 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, moción 48 vía artículo 137., pp. 561-563. El resaltado no pertenece al original.

[264] Artículo 51 del Código Penal: *"La pena de prisión y las medidas de seguridad se cumplirán en los lugares y en la forma en que una ley especial lo determine, de manera que ejerzan sobre el condenado* ***una acción rehabilitadora****..."* (resaltado no es del original).

[265] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Expediente 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Sesión ordinaria N.º 8 CESN, 24-08-10, p. 585, se le agradeció la participación a: Francisco Salas, Adalid Medrano (Procuraduría General de la República), Carlos Chinchilla (ex magistrado) y Juan Marcos Rivero.

ciudadana veinte años vista, donde una de las materias que debe tocarse, entre muchas, es una legislación penal adecuada y vigente, que rija para los próximos años, pero bueno, este país, que no tiene todavía una conciencia de que hay que hacer estructura mucho más allá de lo que se está conociendo de forma inmediata, no ha sido posible tener esa mentalidad. Y es por eso que, bueno, hace tres años o cuatro o dos años un grupo de diputados presentó este proyecto, porque pensó que había que legislar en estas materias y se está legislando, aisladamente, yo estoy de acuerdo, que debería de haber algo integral, pero son temas que no pueden obviarse, son temas que no pueden quedar por fuera de una legislación, sobre todo con los mecanismos que existen en estos momentos para la suplantación, para el robo a través de Internet […] Legislar en esta materia ha sido muy difícil [...] porque es una materia prácticamente nueva, donde en Costa Rica hay pocos expertos..."[266]

El diputado Carlos Humberto Góngora Fuentes, manifestó: *"El artículo 196 actual establece la violación de correspondencia o comunicaciones, y estamos incluyendo la violación de correspondencia y comunicaciones por vía de soporte y sistema informático porque también a muchas personas de forma inescrupulosa envían correos solicitando información, actualización bancaria, y demás datos, y aprovechan esas comunicaciones que pareciesen ser oficiales y transparentes para vaciar las cuentas bancarias de la gente, detrás de esta legislación hay rostro humano, gente que ha visto cómo sus ahorros de toda una vida le son arrancados vilmente por otro que es muy diestro y muy capacitado en la telemática, en la informática, eso es lo nuevo que estamos incluyendo..."*[267] Nótese nuevamente que, existió en la discusión legislativa una confusión en cuanto a tipificar conductas, precisamente porque el hecho de que exista el *"phishing"* no quiere decir que tal conducta no estaba sancionada en nuestra legislación. Señala

[266] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, acta N.º 89, 11-10-2010., pp. 658-660.

[267] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, acta N.º 89, 11-10-2010., p. 665.

además, dicho ex legislador *"...ya no necesitan robarle a usted la billetera disimuladamente sin imponer fuerza, le roban – como he dicho- su dinero a través de las tarjetas magnéticas o dispositivos electrónicos, por usted, muy confiadamente, va y paga la gasolina, y cuando pasan su tarjeta por el lector están duplicando la información de barras que tiene su tarjeta y, entonces, usted ni siquiera se da cuenta, y así vacían hasta el límite insoportable su tarjeta de crédito..."*[268]

Propiamente, en cuanto a la pena del delito de la estafa informática, el diputado Fishman dijo: *"Cuando se habla de sanciones penales, no es posible entender que la sanción penal pueda ser la misma para una estafa ordinaria, que para una estafa informática, su contenido es distinto, su medio de utilización, que su medio informático es mucho más sofisticado y, además de eso, es un medio para estafar sumamente peligroso. Esto nos da, en este aspecto, una connotación distinta a la que nosotros queremos regular y queremos proteger también, de ahí que el proyecto pretenda penas altas de prisión."* Asimismo, sin citar ninguna fuente, dicho diputado manifestó: *"Actualmente, la mayoría de las amenazas cibernéticas que tenemos tienen como una mezcla entre lo que se comete en el país y lo que se comete utilizando servidores internacionales; en realidad, el noventa por ciento de los delitos informáticos que se ejecutan vienen de personas que se encuentran dentro de la propia empresa y que, a la vez, tienen acceso a la base de datos o a la información que maneja propiamente la empresa, de allí la necesidad de tipificar una serie de delitos y de sancionarlos con penas superiores a los delitos convencionales, porque ahí se está aprovechando de la confianza de tener acceso a cierta información, que es una cosa todavía peor que el delito de la estafa común y corriente..."*[269] De los comentarios anteriores se evidencia que, efectivamente quienes crearon la ley, entendieron la estafa informática como una

[268]ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, acta N.º 89, 11-10-2010., p. 665.

[269] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 "Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos", acta N.º 89, 11-10-2010., pp. 668 y 669. El subrayado no corresponde al original.

estafa modernizada, por lo tanto, fijaron en abstracto una pena mayor que la estafa convencional, dejando de lado que, esta última tiene relación directa con un engaño hacia un ser humano, extremo que a nuestro criterio, tal y como se expuso en capítulos anteriores, resulta más reprochable.

Señala Fishman: *"En el caso del sistema financiero, en el caso de los bancos, recordemos tres casos puntuales que se dieron, hace pocos meses hubo un fenómeno de suplantación de sitios web, donde aparecían web gemeleados de los bancos y llevaban a los clientes a introducir nuevamente sus datos bancarios y sus claves de acceso a las cuentas y así se presentaba todo el daño al sistema financiero y al daño, por supuesto, a los clientes, es decir, el gemeleo. En segundo caso, y creo que es muy conocido por todos, y se ha llevado a los tribunales de justicia, fue el caso del Phishing, en donde también causó muchísimo perjuicio a los ciudadanos y también a las instituciones financieras. Y un tercero, talvez de hace más años, que fue el caso de la corrida que sufrió el Banco de San José, que fue una corrida que un solo día a un banco le sacaron, mediante la utilización de los medios informáticos, cualquier cantidad de millones de dólares, que si no hubiera sido por la solvencia del banco este hubiera quebrado..."*[270]

Producto de lo anterior, la Asamblea Legislativa envió consulta a la Corte Suprema de Justicia, para que emitiera criterio con respecto al proyecto de ley sustitutivo tramitado bajo el expediente 17.613, dicho trámite le fue encargado a Carlos Chinchilla[271], lo que llama la atención, en tanto que, fue él quien precisamente defendió el proyecto ante el Poder Legislativo, es decir, desempeñó doble rol en el proceso de redacción de la ley.

Como primer aspecto, Chinchilla indica en su informe: *"Cuando hablamos de la **ciberdelincuencia**, realizamos una directa identificación con los llamados*

[270] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, acta N.º 89, 11-10-2010., p. 669.

[271] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., pp. 698-714.

***delitos económicos**. Estos último desde el ámbito de la **criminalidad informática**, muestran una característica que los identifica singularmente, referida a la utilización de las modernas **Tecnologías de la Información y la Comunicación** (en adelante **TIC**), en medio de la llamada **Sociedad de la Información y el Conocimiento**. Una característica relevante de estos delitos, como lo veremos, se refiere a la utilización de los llamados **delitos de peligro abstracto**, donde no se necesita la existencia de un resultado, sino, por el contrario, el ordenamiento adelanta la protección de bienes jurídicos que consideran relevantes, para sancionar la acción delictiva. Por ello, lo que hoy identificamos como tentativa en los delitos de resultado, en los delitos de peligro, sería la verificación de un riesgo o peligro y, por lo tanto, sancionable como si se tratara del resultado mismo. Lo dicho, corresponde a la figura de los delitos de peligro abstracto."*[272] Agrega que *"Los delitos económicos, así como los delitos informáticos, tienen mucho que ver, con la evolucionada **delincuencia organizada**. Donde poderosas organizaciones criminales se sirven de muchas personas, para cometer delitos informáticos."*[273]

Llama la atención el siguiente comentario realizado por Chinchilla: "*En la delincuencia informática, partimos de que se puede cometer bajo el supuesto de la acción ejecutada con dolo, lo que corresponde a que el sujeto activo cuenta con el debido conocimiento y voluntad, o, según sea el caso, con culpa o imprudencia, identificada por la infracción al deber de cuidado."*[274], y es que si se observa el proyecto de ley, en ningún momento se contempló algún delito en modo de comisión culposa. También, el abogado realizó una afirmación sin mayor sustento

[272] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 699. El resaltado pertenece al original.

[273] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 700. El resaltado pertenece al original.

[274] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 701.

probatorio al decir: *"...en la práctica, la mayoría de delitos informáticos son cometidos por personas que no tienen esos profundos conocimientos en informática..."*[275] Esa afirmación se contrapone por completo, con lo dicho por el profesor Francisco Castillo, cuando señaló: *"...En Costa Rica carecemos de estudios sobre el perfil del estafador informático y de estadísticas fiables sobre la estafa informática..."*[276] Al momento de realizar la presente investigación, se corrobora la indicado por el jurista Castillo, y no lo dicho por el abogado Chinchilla.

De igual manera, a criterio de Chinchilla, el ordinal 196 bis del CP, denominado violación de datos personales, protege la privacidad y la intimidad, de acuerdo con el principio de la autodeterminación informativa.[277]

En cuanto al hurto agravado, numeral 209 del CP, señaló Chinchilla: *"Se trata del delito de **Hurto agravado**, donde se modifica la numeración de los incisos para establecerlos en orden alfabético, su contenido queda igual y establece una nueva penalidad de 1 a 9 años de prisión si el valor de lo sustraído no excede de 5 veces el salario base y, si es mayor a esa suma, la penalidad se mantiene de 5 a 10 años. La sensible novedad que se introduce en esta norma, se refiere al inciso c), cuando se introduce la utilización de **"claves de acceso, tarjetas magnéticas o dispositivos electrónicos"**. Con ello, se produce un sensible avance en la legislación de los delitos informáticos, **pues esta conducta ha traído un grave problema de resolución por parte de los Tribunales de Justicia y la misma Sala Tercera, donde se ha llegado a discutir la subsunción de la conducta delictiva en el delito de estafa informática, hurto agravado o hurto simple. Con esta reforma, no quedará duda que la***

[275]ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 701.

[276] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 52.

[277] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 704.

utilización delictiva de estos instrumentos de carácter informático, se considerarán hurtos agravados.*"*[278]

En ese sentido, ante una consulta legislativa facultativa de constitucionalidad interpuesta por las diputaciones José María Villalta Florez-Estrada y otras, la Sala Constitucional emitió el voto N.º 2011-992 de las 15:47 h del 26 de enero de 2011, resolución en la cual mencionó con respecto a dicho proyecto sustitutivo de ley: *"...En efecto, el resultado del agravamiento de la sanción privativa de libertad afecta no solo la disposición conexa con delincuencia informática, sino también los demás supuestos del artículo. Se busca aumentar el extremo superior de la sanción de cinco a nueve años de prisión, si el valor de lo sustraído no excede de cinco veces el salario base, y pasaría el extremo inferior de un año a cinco años, cuando el hurto superara la suma indicada, vedando con ello la aplicación del beneficio establecido en el artículo 59 del Código Penal. De este modo, las conductas que quedarían más severamente sancionadas comprenderían hurto de cabezas de ganado mayor o menor, aves de corral, productos o elementos que se encuentren en uso para explotación agropecuaria; hurto aprovechando las facilidades provenientes de un estrago, de una conmoción pública o de un infortunio particular del damnificado; hurto con uso de ganzúa, llave falsa u otro instrumento semejante, o de la llave verdadera que hubiere sido sustraída, hallada o retenida; hurto de equipaje de viajeros, en cualquier clase de vehículos o en los estacionamientos o terminales de las empresas de transportes; hurto de vehículos dejados en la vía pública o en lugares de acceso público; hurto de cosas de valor científico, artístico, cultural, de seguridad o religioso, cuando, por el lugar en que se encuentren estén destinadas al servicio, a la utilidad o a la reverencia de un número indeterminado de personas, o librados a la confianza pública; y hurto cometido por dos o más personas. El único común denominador entre todas estas clases de hurto y el tema de la iniciativa es constituir material penal, límite demasiado laxo, constitucionalmente hablando. Bajo una técnica*

[278] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 704. El resaltado pertenece al original.

similar, bastaría con la sola inclusión de alguna circunstancia relacionada con el tema de la iniciativa, para variar las sanciones concernientes a grupos de conductas, no necesariamente del mismo eje temático. En una democracia, flexibilizar a tal punto la regulación de la materia penal, es, cuando menos, contraproducente. Concluye la Sala, por lo tanto, que se lesiona también en este caso el principio de conexidad, y con ella la Constitución. Según se advirtió supra, por configurar un vicio esencial en el procedimiento legislativo, la decisión de este Tribunal es de acatamiento obligatorio pata (sic) la Asamblea Legislativa..."[279]

Haciendo un análisis en retrospectiva, en cuanto a dosificación de penas, tenemos que cuando el ex magistrado Chinchilla defendió el proyecto de ley, consideró apropiada la reforma al hurto agravado, con las siguientes penas: de 1 a 9 años de prisión (objeto sustraído no excediera del valor equivalente a 5 veces el salario base) y de 5 a 10 años de prisión (objeto sustraído exceda el valor de 5 veces el salario base) en los casos en que se utilice para el hurto "claves de acceso, tarjetas magnéticas o dispositivos electrónicos" (recuérdese que esa reforma del numeral 209 del CP no fue aprobada, sin embargo, el magistrado le dio el visto bueno).

Ahora bien, la reforma aprobada al 217 bis, prevé una sanción de 3 a 6 años de prisión en la modalidad simple de comisión, y una agravante de 5 a 10 años de prisión. Es decir, si comparamos aquella reforma propuesta al 209 (no aprobada) con la verdaderamente aprobada al 217 bis, el extremo mínimo pasó 1 a 3 años de prisión, sin hacerse un análisis exhaustivo, ni en la discusión legislativa, ni tampoco en el criterio vertido por el ex magistrado Chinchilla en representación de la Corte Suprema de Justicia. También es interesante que, en el criterio emitido por Chinchilla, utilizó el concepto de "estafa informática", ello a pesar de que, para esa data, evidentemente la reforma del 217 bis no estaba aprobada, es decir, no existía la "estafa informática" como tal. Él mencionó que la

[279] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Sala Constitucional, voto N.º 2011-000992 de las 15:47 h del 26-01-2011, pp.817 y 818.

reforma del 209 del CP iba a permitirle a la Sala Tercera solucionar el problema de subsunción de las conductas en las que se utilizaran *"claves de acceso, tarjetas magnéticas o dispositivos electrónicos"*, propiamente relacionado con los delitos de "*estafa informática, hurto agravado o hurto simple"*, indicó de manera categórica: *"...Con esta reforma, no quedará duda que la utilización delictiva de estos instrumentos de carácter informático, se considerarán hurtos agravados..."*[280] Otro aspecto que no se puede omitir es que, esa reforma al artículo 209, estaba contemplada dentro del mismo proyecto de ley que reformó el 217 bis, que tal y como se verá, después de que Chinchilla emitió el informe de aprobación al proyecto de ley, la redacción del 217 bis mantuvo exactamente la misma redacción en su contenido, únicamente que Chinchilla promovió cambiarle el título. Es decir, que el informe positivo del para entonces magistrado, permitía que una misma conducta sea la utilización de *"claves de acceso, tarjetas magnéticas o dispositivos electrónicos"*, pudiese encuadrar en cualquiera de los dos tipos penales. En ese sentido vale mencionar que, en la respuesta emitida por el magistrado a la Asamblea Legislativa, no se hizo ningún tipo de crítica o cuestionamiento al respecto.

En lo referente a la redacción del artículo 217 bis de fraude informático, señala Chinchilla que: *"La reforma en su contenido ha sido muy bien pensada, debido a que se incluyen dos elementos esenciales; uno referido a la **"manipulación"** como verbo identificador de la conducta delictiva, junto con el de **"influir"** y, otro, donde se introduce la posibilidad de que las acciones defraudatorias se realicen al momento del **ingreso** de los datos al sistema, siendo que el actual artículo 217 bis del Código Penal, sobre el Fraude informático, no se contemplan estos dos elementos. Los llamados **"insiders"** o la manipulación en el ingreso de los datos, según estadísticas a nivel internacional, es donde se verifican, aproximadamente, el 80% de todas las estafas informáticas; además, se mantiene en la descripción del tipo penal, la manipulación en el **procesamiento***

[280] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Expediente 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 704.

*de los datos y el **"outsiders"** o **salida** de los datos. Estos tres momentos son los que corresponden al funcionamiento de cualquier sistema informáticos (sic), donde los mismos se alimentan de datos o información (introducción), se procesa la misma y, por último, se da la salida de los datos. Un aspecto que no resulta especialmente esencial y no afecta para nada el contenido del tipo penal, pero sí es importante para su correcta identificación, se refiere al **nomen iuris** otorgado al artículo 217 bis del proyecto, al identificarlo como **Fraude informático**, al igual que la norma vigente hoy día. En realidad, el error de ese artículo en su nombre jurídico que mantiene actualmente, se repite en el actual proyecto de ley, cuando en realidad se debió adoptar el nombre de **Estafa informática**. En este sentido, para explicar nuestra posición, es importante aclarar que, cuando en la doctrina de los Delitos Informáticos se habla de "fraude", no es lo mismo que, cuando en la doctrina del Derecho Penal se refiere al mismo término "fraude". Con ello se quiere decir que, en delitos informáticos el concepto de "fraude" va más allá que en el Derecho Penal especial. Existe confusión entre los conceptos de fraude informático y estafa informática. Por eso podemos decir que, no es lo mismo fraude informático y estafa informática, aunque ambos se llegan a confundir; donde los fraudes informáticos constituyen el género y las estafas informáticas, son la especie. Por ello, podríamos afirmar que, "toda estafa informática es un fraude informático, pero no todo fraude informático es una estafa informática". En realidad, si se revisa la doctrina acerca de los delitos informáticos, muchas veces un fraude informático puede ser un hurto informático, un sabotaje informático o un daño informático. Por ello, limitar el **nomen iures** (nombre que se le da un delito) (sic) para ubicar su contenido, como lo podría ser el fraude informático, no resulta correcto en el presente caso, lo más apropiado sería renombrarlo como **Estafa informática**".*[281] Tal planteamiento, tuvo tres votos favorables de los únicos tres diputados presentes el 06 de diciembre de 2010, cuando en la Comisión Permanente Especial de Redacción de la Asamblea Legislativa, se decidió

[281] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 705.

cambiar el nombre al tipo penal[282]. Nótese que, el planteamiento omitió por completo mencionar por qué a pesar de que la descripción del 217 bis no obedece a una “estafa”, se le debe denominar de esa manera.

Relacionado con el tema de la estafa informática, pero propiamente en lo que respecta al numeral 233 del proyecto, delito denominado suplantación de páginas electrónicas, el señor Chinchilla indicó *“Se recoge en forma específica, lo relativo a las conductas del “**phishing**” y el **pharming**”, las cuales han afectado y lesionado a muchas personas alrededor del mundo. Son actuaciones de especial actualidad, donde constantemente se verifica una gran cantidad de conductas fraudulentas, por medio de las cuales se afecta económicamente a una gran cantidad de personas, empresas e instituciones. En este artículo se impone pena de prisión de 1 a 3 años a quien en perjuicio de un tercero, suplante sitios legítimos de la red de Internet y, además, se agrava la pena de 3 a 6 años de prisión, cuando a consecuencia de esa suplantación capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.”*[283]

El magistrado Chinchilla en el documento de visto bueno al proyecto de ley, consideró oportuno sancionar con pena de prisión de 1 a 3 años, aquella persona que *“en perjuicio de un tercero, suplante sitios legítimos de la red de Internet”* (primer párrafo, artículo 233 del CP). Nótese que, con esa redacción existe una anticipación a las barreras de punibilidad, situación muy peligrosa en un Estado Democrático y de Derecho como el costarricense, además, de que riñe con el Derecho Penal de acto. Con afán de sancionar cualquier comportamiento humano, se decidió penalizar hasta la misma fase de ideación de acuerdo con el *iter criminis*. En el segundo párrafo del artículo 233 del CP, se sanciona con una pena

---

[282] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. COMISIÓN PERMANENTE ESPECIAL DE REDACCIÓN. Exp. 17.613 *“Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos*”, sesión ordinaria N.º 33, 06-12-10., pp. 748 y 749.

[283] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. COMISIÓN PERMANENTE ESPECIAL DE REDACCIÓN. Exp. 17.613 *“Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos*”, sesión ordinaria N.º 33, 06-12-10., p. 708.

de 3 a 6 años de prisión: *"cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero."* Definitivamente la redacción actual de dicho numeral amerita una investigación aparte, ya que existe una relación directa con la denominada estafa informática.

Como conclusión, Carlos Chinchilla[284] emitió un dictamen positivo del proyecto sustitutivo a la Asamblea Legislativa, afirmó que la mayoría de las penas

---

[284] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 712, en cuanto a un tema que no se puede invisibilizar, el ex magistrado mencionó: *"El ARTÍCULO 4 de este proyecto, se dirige a modificar el Artículo 8 de la Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones y sus reformas, N.º 7425 del 9 de agosto de 1994, que permite la autorización de intervenciones introduciendo la posibilidad de los Tribunales de Justicia de autorizar las intervenciones de comunicaciones orales, escritas o de otros tipo (sic), incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de delitos informáticos o cometidos mediante la utilización de medios informáticos, electrónicos, telemáticos, ópticos o magnéticos, los demás delitos se mantienen incólumes. Esta reforma resulta de vital importancia, al introducir la posibilidad de autorizar la intervención de comunicaciones cuando involucre esclarecer delitos informáticos o cometidos por medio de la utilización de las TIC […] Esta reforma mantiene, como siempre ha sido, la obligatoria intervención de los Tribunales de Justicia (Juez Penal o de Garantías), para decidir acerca de la autorización o no, respecto a la intervención de las comunicaciones. Como vemos, le corresponde a un Juez Penal de la República, decidir si procede o no, la intervención de las comunicaciones solicitada en una investigación criminal dirigida por el Ministerio Público. Esta es una facultad de carácter jurisdiccional, otorgada y protegida bajo reserva legal calificada, conforme el artículo 24 de la Constitución Política."* Por otro lado, la Sala Constitucional en el voto N.º 2011000992 de las 15:57 h del 26-01-2011, respecto a ese tema indicó: *"El cambio podría entenderse atinente a la iniciativa bajo una interpretación más que extensiva de ese acto del trámite parlamentario, argumentando que versa, en general, sobre delitos informáticos o cometidos mediante la utilización de medios informáticos, electrónicos, telemáticos, ópticos o magnéticos. Sin embargo, a juicio de la Sala, se incurrió en un exceso en el ejercicio del derecho de enmienda, al vincular esa alusión genérica a la materia tratada en la iniciativa con la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales. El derecho a la intimidad y, concretamente, a la libertad y secreto de las comunicaciones, está celosamente regulado en la Constitución Política (artículo 24), al punto que es uno de los pocos derechos fundamentales respecto de los cuales se dejó patente, en la propia Carta Fundamental, la característica de la imposición de restricciones únicamente en casos excepcionales y justificados, a través de norma de rango legal especial y aprobada por mayoría calificada. La disposición constitucional es casi reglamentaria al estipular que esa ley especial debe precisar los casos en que procede la intervención de comunicaciones, que ella solamente puede ordenarla un órgano jurisdiccional, por delitos expresamente enlistados y por un tiempo limitado. Así las cosas, valerse de la iniciativa de una ley ordinaria, para introducir tardíamente una modificación a la ley especial que ampara el artículo 24 constitucional constituye un ejercicio abusivo e inconstitucional del derecho de enmienda. De nada vale que en la Constitución se salvaguarde este derecho fundamental con disposiciones de procedimiento parlamentario extraordinarias, si ellas se echan por tierra con la adopción de disposiciones, de última hora, propias de la ley especial indicada. Por las anteriores*

en sus extremos menores son de 3 años lo cual permite salidas alternas al proceso, e indicó que se trata de un proyecto de ley "novedoso" que colocaba a Costa Rica para aquel entonces, como uno de los países más avanzados del área en dicha temática, ya que así se combatiría la cibercriminalidad.[285]

Vale recalcar el comentario realizado por la diputada Carmen María Muñoz Quesada, quien indicó que las penas planteadas en el proyecto de ley N° 17.613 eran desproporcionadas, negando por ejemplo la suspensión del proceso a prueba, literalmente señaló: *"Pero insistimos que este proyecto, así como está presentado, muestra una suerte de desprecio también por la dignidad humana y una negación de las oportunidades procesales [...] que la pena per se, no soluciona los problemas de fondo."* A pesar de esa manifestación, el proyecto fue votado en primer debate el 30 de noviembre de 2010, mediante el acta N.º 117, con 32 votos afirmativos y 12 negativos.[286]

Posteriormente, y debido a una consulta facultativa de constitucionalidad presentada el 09 de diciembre de 2010 por el diputado José María Villalta Florez-Estrada y otras personas legisladoras, la Sala Constitucional mediante la resolución ya mencionada N° 2011-992 de las 15:47 horas del 26 de enero de 2011, resolvió por criterio de mayoría (Ana Virginia Calzada M., Rosa Esmeralda Blanco, Roxana Salazar C., y Enrique Ulate C): *"Se evacua la consulta en el sentido que el proyecto de Ley de "Reforma a varios artículos del CP y adición de una nueva sección VIII denominada "Delitos informáticos y conexos" al título VII*

---

razones es que se considera inconstitucional la inclusión, en el texto sustitutivo aprobado en el último informe de la comisión dictaminadora de mociones planteadas vía artículo 137 del Reglamento parlamentario, de una norma que modifica el artículo 9° de la Ley #7425. Al tratarse de un vicio en el procedimiento legislativo, la decisión de la sala resulta vinculante, según lo establece el artículo 101 de la Ley de la Jurisdicción Constitucional" (ver expediente legislativo N° 17.613, pp. 815 y 816).

[285] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Informe de la Corte Suprema de Justicia, Poder Judicial, 27-10-10., p. 713.

[286] ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*, 30-11-2010., p. 729.

del Código Penal", que se tramita en el expediente legislativo número 17.613 es inconstitucional, en cuanto al procedimiento, por haber infringido el principio de conexidad..."[287]

Producto de lo anterior, el expediente se devolvió a la Asamblea Legislativa, de esa manera, la denominada Comisión Permanente Especial de Consultas de Constitucionalidad, emitió un dictamen señalando que se debía remitir el expediente para que se sometiera ***"la iniciativa de marras al trámite de votación en primer debate, después de eliminar del texto del proyecto de ley las mociones declaradas inconexas****..."*[288] De manera unánime las diputadas y diputados, estuvieron de acuerdo con el informe de la Comisión *supra* citada. No sin antes mostrar disconformidad con el voto de la Sala Constitucional, siendo que el diputado Luis Fishman indicó: *"...dice el diputado Villalta de la maravilla de tener a la Sala por detrás y que, por dicha, que nos salvaron la tanda […] Pero de todos los que dictaminan aquí […] nadie ha mencionado del que, realmente, conoce de Derecho parlamentario, el voto salvado del doctor Fernando Castillo […] se aparta de lo que dice la mayoría de los magistrados, que no conocen de nada del Derecho parlamentario..."*[289] Secundado por la manifestación del diputado Luis Gerardo Villanueva Monge, quien señaló: *"...la Asamblea tiene que llegar a eso, hay que enseñarle a la Sala Constitucional […] Derecho Parlamentario.*

---

[287] Existieron dos votos salvados: el primero de ellos perteneciente a los magistrados Gilbert Armijo Sancho y Fernando Cruz Castro, relacionados con la mayoría necesaria para la aprobación del texto en primer debate; el segundo, emitido por el magistrado Fernando Castillo Víquez, quien declaró que el proyecto de ley no contenía ningún vicio de procedimiento.

[288] ASAMBLEA LEGISLATIVA. DEPARTAMENTO DE SERVICIOS TÉCNICOS. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Oficio N.º CON.007-2011C, 16-02-11, el cual es una aclaración del oficio N.º CON.006-2011C, 15-02-2011., pp. 838 y 839. El resaltado pertenece al original.

[289] ASAMBLEA LEGISLATIVA. DEPARTAMENTO DE SERVICIOS TÉCNICOS. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Acta de sesión plenaria N.º 153, 07-03-2011., p. 897.

Desgraciadamente ellos han sido parte de la atrofia parlamentaria costarricense..."[290]

El 28 de abril de 2011, la Comisión Especial de la Asamblea Legislativa, planteó una moción[291] en el proyecto de ley N.º 17613, mediante la cual el numeral 217 bis, pasó a denominarse "estafa informática", y el contenido varió a la redacción actual. Posteriormente, la Comisión Permanente Especial de Consultas de Constitucionalidad emitió el informe unánime afirmativo, mediante el cual mantuvo exactamente el mismo proyecto de ley discutido en la primera ocasión, eliminando únicamente la reforma del numeral 209 del CP y el artículo 9 de la ley N.º 7425.[292] De igual manera la Comisión Permanente Especial de Redacción, el día 04 de junio de 2012, emitió la redacción final del citado proyecto[293], con la redacción vigente del 217 bis.

Ahora bien, propiamente en lo que se refirió a la discusión en segundo debate, en el plenario las personas diputadas, entre ellas Óscar Gerardo Alfaro Zamora mencionó como justificante de la aprobación de la ley: *"De esta forma, no es extraño que los malhechores busquen nuestra información para estafarnos directamente, o para utilizarla y de esa forma hacerse pasar como si fueran nosotros en la misma red o en escenarios reales. Así fácilmente pueden afectar nuestros estados bancarios y también los sociales […] Al mismo tiempo estamos seguros que al aprobar esta ley, estaremos contribuyendo a la seguridad de las*

---

[290] ASAMBLEA LEGISLATIVA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Acta de sesión plenaria N.º 153, 07-03-2011., p. 900.

[291] ASAMBLEA LEGISLATIVA. Expediente 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. p. 938 y 941.

[292] ASAMBLEA LEGISLATIVA, COMISIÓN PERMANENTE ESPECIAL DE CONSULTAS DE CONSTITUCIONALIDAD. Exp. 17.613 *"Reforma a varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, y al Título VII del Código Penal"*, 28-04-2011., pp. 959-970.

[293] ASAMBLEA LEGISLATIVA, COMISIÓN PERMANENTE ESPECIAL DE CONSULTAS DE CONSTITUCIONALIDAD. Exp. 17.613 *"Reforma a varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, y al Título VII del Código Penal"*, 04-06-2012., pp. 1017-1025.

personas, que podrán estar más tranquilas, pero que especialmente, tendrán la posibilidad defenderse (sic) de quienes roban una identidad en la red, de quienes ofenden, de quienes suplantan páginas de internet, de quienes hacen inservibles los equipos de computo (sic) *con la propagación de un virus informático, y que la impunidad en estos casos ya no sea la norma, sino la excepción..."* [294]

El diputado Flórez-Estrada, indicó: *"Había otros temas inconexos como, por ejemplo, el incremento de la pena de todos los delitos de hurto a unos que no tenían nada que ver con la materia informática, apenas que puedan calificarse –así lo consideramos- como desproporcionadas. Eso también se eliminó pero con un error, porque se eliminó toda la reforma al delito de hurto agravado, y, en realidad, lo que había que aclarar era que el aumento de las penas, o la pena más alta, no regía para todos los otros supuestos de ese tipo penal. En realidad, lo que pretendía la versión original del proyecto era abrigar una nueva modalidad de hurto, el hurto que se comete utilizando una llave o dispositivo electrónico. Ese aspecto se eliminó del proyecto, aunque no debía de haberse eliminado, por una decisión no totalmente acertada, en cuanto a los objetivos del voto de la Sala Constitucional, en la Comisión de Consultas de Constitucionalidad."*[295] Propiamente, en lo que respecta al delito de estafa informática, el argumento del diputado fue el siguiente: *"Otros aspectos importantes de este proyecto es la regulación de los delitos económicos cuando se usan medios informáticos; la extorsión a través de medios informáticos, la estafa informática. Hoy en día, no hace falta palabrear, engañar en persona a un ciudadano para estafarlo, muchas veces estas estafas se cometen de forma totalmente impersonal, utilizando un correo electrónico, accesando (sic) indebidamente una clave electrónica, bueno,*

[294] ASAMBLEA LEGISLATIVA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Acta de la Sesión Plenaria N.º 23, 07-06-2012, p. 1035.

[295] ASAMBLEA LEGISLATIVA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Acta de la Sesión Plenaria N.º 23, 07-06-2012, pp. 1036 y 1037.

eso hace falta regularlo correctamente..."[296] Además, finalizó la intervención visibilizando el tema de las penas, las cuales realmente no fueron estudiadas a profundidad: *"faltó tal vez hacer un estudio mayor sobre la proporcionalidad de las penas, más integral respecto a todo el Código Penal, para que las penas de estos delitos sean verdaderamente proporcionadas con otros tipos penales de igual o similar gravedad, donde se lesiona un mismo bien jurídico, hay discordancias respecto a los montos de las penas establecidos en esta ley, y otros tipos penales que regulan conductas de igual o menor gravedad, inclusive, bueno, eso lo planteamos en la consulta por el fondo a la Sala Constitucional, la Sala no se pronunció sobre ese tema porque encontró vicios de procedimiento […] salvo ese aspecto podemos decir que si comparamos el proyecto que entró, el proyecto original y lo que sale de esta Asamblea Legislativa, con los aportes de la Corte, con aportes de expertos, con aportes de muchas diputadas y diputados de este Plenario, realmente hay una mejor ley para regular esta materia..."*[297]

Después de realizada la discusión legislativa, en la cual únicamente intervinieron 3 diputados (José Roberto Rodríguez Quedada, Oscar Gerardo Alfaro Zamora y José María Villalta Flórez-Estrada), se procedió a la votación en segundo debate, recibiendo 40 votos a favor de las 40 personas diputadas presentes, decreto legislativo N.º 9048.[298] De esa manera y con su respectiva publicación en el Diario La Gaceta, se convirtió en ley de la República.

En realidad, el problema de fondo en cuanto a los verbos influir y manipular, así como el uso de datos falsos, incompletos o indebidos, del delito de estafa informática, no fueron analizados por el legislativo al momento de promulgar el

---

[296] ASAMBLEA LEGISLATIVA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Acta de la Sesión Plenaria N.º 23, 07-06-2012, p. 1038.

[297] ASAMBLEA LEGISLATIVA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Acta de la Sesión Plenaria N.º 23, 07-06-2012, p. 1038.

[298] ASAMBLEA LEGISLATIVA. Exp. 17.613 *"Reforma a varios artículos del CP y adición de un nuevo capítulo denominado delitos informáticos"*. Acta de la Sesión Plenaria N.º 23, 07-06-2012, pp. 1039 y 1045.

actual artículo 217 bis del CP, las discusiones giraron en torno a criterios punitivistas y alarmistas.

Producto de todo lo anterior, se modificó el artículo 217 bis del CP, de seguido se realiza un cuadro comparativo entre ambas figuras penales:

Tabla 6. *Comparación entre fraude y estafa informática*

Fraude informático. Antiguo art. 217 bis del Código Penal (Ley N° 8148 de 24 de octubre de 2001, publicado en La Gaceta de 21 de noviembre de 2001)	**Estafa informática. Actual art. 217 bis del CP** (Ley N° 9048 del 10 de julio de 2012, publicada en el Alcance 172 a La Gaceta N° 214 del 06 de noviembre de 2012)
"Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema." (Subrayado no corresponde al original).	*"Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.* *La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos."*

La primera modificación es referente al rango de penas previstas en abstracto, la cual estaba prevista de 1 a 10 años de prisión en el fraude informático, y pasó a una pena de 3 a 6 años de prisión en la que podemos denominar “estafa informática simple”, es decir, aumentó el extremo menor de la pena, pero disminuyó el mayor en ese modo de comisión. Sin embargo, el nuevo tipo penal incorporó una nueva modalidad agravada de comisión, la cual podemos denominar “estafa informática agravada”, previendo una pena de prisión en abstracto que oscila entre los 5 a los 10 años de prisión. A grandes rasgos se determina entonces que, el legislador decidió aumentar el extremo menor de la pena, que pasó de 1 año de prisión a 3, mientras tanto el extremo mayor de los 10 años de prisión no sufrió alteración.

Otra diferencia es que, el delito de estafa informático incorporó el verbo “manipular”, ausente en el fraude informático. Asimismo, mantuvo el verbo “influya”, pero agregó la siguiente frase: “influya en el ingreso”. En ese sentido el TASPIICJSJ, en el voto 2015-0738 de las 09:05 horas del 22 de mayo de 2015, mencionó: *“…La estafa informática, amplió su configuración típica, al incluir acciones que no estaban en aquel otro delito, porque integró la acción de "manipular o influir en el ingreso" pero mantuvo el "influir en el procesamiento o en el resultado de los datos". Asimismo, para los casos en que se trate de sistemas de información bancaria, como es este asunto, elevó la pena mínima, a cinco años de prisión, (párrafo segundo del artículo 217 bis del Código Penal), en lugar del año que tenía como extremo menor, el derogado fraude informático […] Es así cómo, el fraude informático se cometía, cuando el sujeto activo: "influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante... uso indebido de datos". Lo anterior implica que, tanto se puede influir en el procesamiento, como en el resultado de los datos, de un sistema de computo (sic)…”*

De acuerdo a todo lo anterior, se puede indicar que el legislador previó en el primer párrafo, la posibilidad de que la acción sea realizada por cualquier persona, es decir, se podría catalogar el delito de estafa informática como un

“delito común”. Sin embargo, se podría considerar este delito también como un “delito especial impropio”, ya que en el segundo párrafo estableció una agravante en razón de las condiciones del autor, propiamente en los casos en que, la acción la lleven a cabo los empleados encargados de administrar o de dar soporte a los sistemas de computación.

En resumen, de las discusiones legislativas no se evidenció un análisis exhaustivo del delito de estafa informática, no se analizó qué acontece en otros países al respecto. Inclusive, no existieron asesorías de personas profesionales en informática que brindaran una orientación en cuanto a la materia, ello a pesar de que, como lo dijimos al inicio de este capítulo, incorporar la informática al derecho es una tarea no convencional, por ende, complicada. Tampoco se hizo un estudio completo y serio de por qué el delito de fraude informático debía ser modificado, no se dijo si con la antigua redacción del numeral 217 bis estaban despenalizadas conductas, ello a pesar de que el artículo siempre ha sancionado a quien influya en un sistema informática por medio del uso de datos falsos, incompletos o indebidos.

Capítulo IV. Tratamiento jurisprudencial de la estafa informática en Costa Rica durante los años 2014 al 2019

El enfoque empírico es fundamental en esta investigación, esa praxis jurídica de las personas operadoras del derecho en la judicatura, permitirá visibilizar cuál es el verdadero tratamiento de la estafa informática en nuestro país.

El período de análisis abarca del año 2014 al 2019; se contemplaron para el estudio resoluciones únicamente de la Sala Tercera de la Corte Suprema de Justicia[299] (STCSJ) y del Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José (TASPIICJSJ).

[299] Vale mencionar que, se analizarán algunas resoluciones anteriores al año 2014 de la Sala Tercera, en razón de haber sido citadas en jurisprudencia del periodo de estudio y también, porque tal y como se verá, la producción en cuanto al tema en dicha Sala de lo penal, ha sido escaso. Otro aspecto necesario de resaltar es que, debido a que la estafa informática entró en vigencia a finales

Resoluciones de STCSJ del año 2012 al 2019

Una vez realizadas las consultas correspondientes en el Centro de Información Jurisprudencial de la STCSJ, Sistema de consulta *"Nexus"*, durante el periodo de estudio, correspondiente a seis años del 2014 al 2019 (inclusive), se obtuvieron un total de veintiún resoluciones diferentes dictadas por la STCSJ, con los siguientes parámetros de búsqueda: *"estafa" "informática"*[300], *"fraude" "informático"* o *"fraude" "informática"*[301] y *"217 bis"*[302]. Es decir, un promedio de 3,5 resoluciones por año, lo cual *prima facie*, demuestra que el tema ha sido poco abordado por dicha Sala de lo penal, ello a pesar de que el tipo penal de estafa informática entró en vigencia desde el año 2012.

Otro aspecto importante es que, a pesar de que existan veintiún resoluciones, no quiere decir que el tópico de estudio se analizó a fondo por parte de la Sala Tercera, ya que trece de esas resoluciones se refieren a

---

del año 2012, las resoluciones de ese año y del 2013 e inclusive algunas posteriores a este último, atienden al tipo penal de "fraude informático" (antiguo 217 bis del CP), esa situación no excluye que en lo que interese, sean utilizadas en la presente investigación.

[300] Los siguientes son los resultados obtenidos con dicho parámetro de búsqueda, año por año, dictadas por la Sala Tercera de la Corte Suprema de Justicia: **Resoluciones: 2014**: Sin resultados; **2015 (dos resultados)**: **1)** Nº 2015-00354 de las 09:55 horas del 27-02-2015 y **2)** Nº 2015-01292 de las 09:28 horas del 16-10-2015; **2016 (un resultado)**: Nº 2016-1025 de las 14:32 horas del 29-09-2016; **2017**: Sin resultados; **2018 (un resultado)**: Nº 2018-00639 de las 09:57 horas del 14-09-2018; **2019 (tres resultados)**: **1)** Nº 2019-00498 de las 18:45 horas del 25-04-2019; **2)** Nº 2019-001501 de las 11:30 horas del 22-11-2019; y **3)** Nº 2019-001591 de las 10:27 horas del 13-12-2019.

[301] Los siguientes son los resultados obtenidos con dicho parámetro de búsqueda, año por año, dictadas por la Sala Tercera de la Corte Suprema de Justicia: **Resoluciones: Año 2014 (6 resultados)**: **1)** Nº 2014-00616 de las 09:05 horas del 04-04-2014; **2)** Nº 2014-01322 de las 10:02 horas del 01-08-2014; **3)** Nº 2014-01563 de las 13:11 horas del 29-09-2014; **4)** Nº 2014-01669 de las 09:48 horas del 17-10-2014; **5)** Nº 2014-01783 de las 15:45 horas del 10-11-2014; **6)** Nº 2014-01909 de las 11:38 horas del 10-12-2014; **año 2015 (3 resultados)**: **1)** 2015-00354 de las 09:55 horas del 27-02-2015; **2)** 2015-00788 de las 11:02 horas del 24-06-2015; y **3)** Nº 2015-01370 de las 08:52 horas del 06-11-2015; y; **año 2016 (4 resultados)**: **1)** Nº 2016-0887 de las 09:39 horas del 09-09-2016; **2)** Nº 2016-01025 de las 14:32 horas del 29-09-2016; **3)** Nº 2016-01081 de las 09:59 horas del 14-10-2016; **4)** Nº 2016-01241 de las 10:15 horas del 02-12-2016; **año 2017 (1 resultado)**: Nº 2017-01097 de las 11:28 horas del 15-12-2017; **año 2018 (2 resultados)**: **1)** Nº 2018-0464 de las 16:25 horas del 20-06-2018; y **2)** Nº 2018-0597 de las 10:32 horas del 31-08-2018; **2019 (1 resultado)**: Nº 2019-0498 de las 18:45 horas del 25-04-2019.

[302] Las resoluciones de la STCSJ obtenidas como resultados con dicho parámetro de búsqueda, estaban contenidas en los anteriores indicadores utilizados.

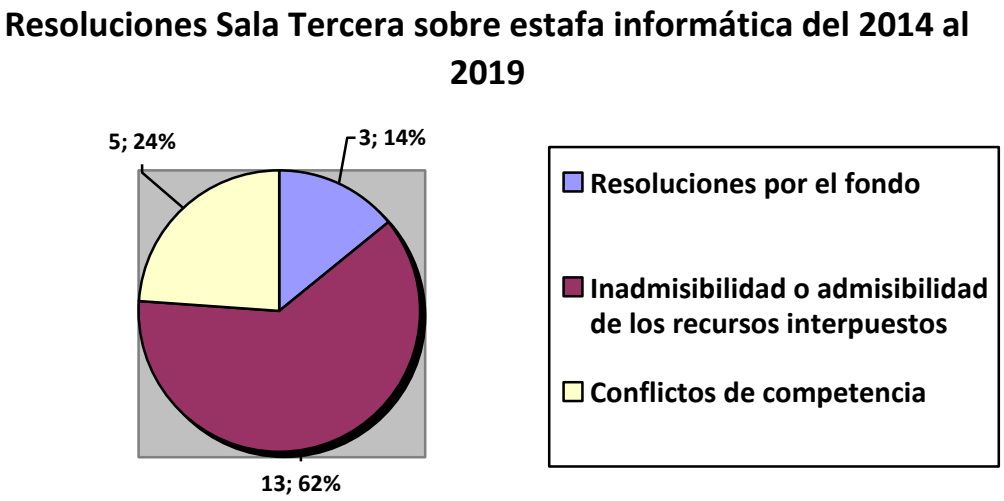
pronunciamientos sobre inadmisibilidad o admisibilidad de los recursos interpuestos[303]; y cinco resoluciones abordaron conflictos de competencia[304]. Es decir, restaría un total de 3 resoluciones en las cuales en realidad el tema no fue estudiado profundamente, tal y como se expondrá. En virtud de lo anterior, siendo poco el material jurisprudencial producido por la STCSJ con respecto al tema de la estafa informática, se procede a hacer una revisión de la totalidad de las resoluciones.

El material jurisprudencial con relación al tema, producido por la STCSJ se puede graficar de la siguiente manera:

[303] Sean las siguientes resoluciones de la STCSJ: **1)** Nº 2014-00616 de las 09:05 horas del 04-04-2014; **2)** Nº 2014-01322 de las 10:02 horas del 01-08-2014; **3)** Nº 2014-01669 de las 09:48 horas del 17-10-2014; **4)** Nº 2014-01783 de las 15:45 horas del 10-11-2014; **5)** Nº 2014-01909 de las 11:38 horas del 10-12-2014; **6)** Nº 2015-00788 de las 11:02 horas del 24-06-2015; **7)** Nº 2015-01370 de las 08:52 horas del 06-11-2015; **8)** Nº 2016-0887 de las 09:39 horas del 09-09-2016; **9)** Nº 2016-01081 de las 09:59 horas del 14-10-2016; **10)** Nº 2016-01241 de las 10:15 horas del 02-12-2016; **11)** Nº 2017-01097 de las 11:28 horas del 15-12-2017; **12)** Nº 2018-0597 de las 10:32 horas del 31-08-2018; **13)** Nº 2019-0498 de las 18:45 horas del 25-04-2019.

[304] Sean las siguientes resoluciones de la STCSJ: **1)** Nº 2015-01292 de las 09:28 horas del 16-10-2015; **2)** Nº 2016-1025 de las 14:32 horas del 29-09-2016; **3)** Nº 2018-0639 de las 09:57 horas del 14-09-2018; **4)** Nº 2019-001501 de las 11:30 horas del 22-11-2019; y **5)** Nº 2019-001591 de las 10:27 horas del 13-12-2019.

Gráfico 2. *Resoluciones STCSJ sobre estafa informática 2014 al 2019*



Ahora bien, después de reflejados los datos estadísticos, se hará alusión a aquellos temas de interés para el presente trabajo, es así como la STCSJ, en la resolución N° 2014-01563 de las 13:11 horas del 29 de septiembre de 2014, al resolver un recurso de casación, se remitió a la resolución N° 148-2006 de las 09:00 horas del 24 de febrero de 2006. En ambos asuntos, la figura penal tratada fue el ya derogado "fraude informático". Si bien, para cuando se emitió la resolución N° 2014-01563 el tipo penal "estafa informática" estaba vigente, lo cierto es que, por la temporalidad de los hechos, ese no era el tipo penal aplicable al caso concreto. A pesar de la situación anterior, ese voto intentó delimitar conceptualmente el delito de "fraude informático".

Podría parecer de poca utilidad para el presente trabajo hacer mención a lo resuelto, sin embargo, se debe recordar que el extinto delito de "fraude informático", tenía una redacción similar a la "estafa informática" en el numeral 217 bis del CP, motivo por el cual, deviene necesario visibilizar cómo éste se interpretaba por parte de la Sala de lo penal: *"…Con respecto a este tipo penal ya la Sala Tercera se ha encargado de delinear el delito informático. En el Voto 2006-148 dijo: "En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea*

como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal)…Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático. De acuerdo a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de incidir en el proceso de los datos del sistema. ***Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema****. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos a seguir, que si alguno se altera fraudulentamente, incidirá en el resto del proceso…"*[305] (el resaltado no corresponde al original).

---

[305] Ver crítica de LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 1ª ed. San José, 2011, pp. 121-122. El autor en su libro, al momento de analizar el delito de "fraude informático", vigente para la época, transcribe exactamente el mismo extracto jurisprudencial (sin especificar el número de resolución, las únicas referencias consignadas son que, se trata de una resolución del año 2006 y de la STCSJ), señala: *"Están hablando, en este caso, de etapas distintas del procesamiento de datos; manipular información, alimentar el sistema, son actos que desde el inicio no están influyendo en el procesamiento, aclárese este concepto; si por ejemplo, en la nómina de pagos de un sistema desde el inicio se modificó un dato de la nómina no se está alterando el procesamiento (la etapa de procesamiento), el equipo informático estará procesando los datos "correctos", según se introdujeron, su proceso es correcto según los datos que se le han dado, se está hablando de la etapa de entrada de datos, no del procesamiento de datos ni del resultado esto es así, porque con base en la función que realiza un sistema de cómputo se tienen cuatro componentes: entrada, procesamiento, salida y almacenamiento […] El artículo habla de influir en el procesamiento o el resultado, por lo tanto, la etapa de entrada no está contemplada en el tipo (la introducción de datos)."* En igual sentido, Carlos Chichilla Sandí, citado por Francisco Castillo en (CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 81): *"Así dice Chinchilla Sandí, 2013, pág. 500: "A lo anterior se une otra crítica relevante, como ya se expuso; primero, el ingreso de los datos-insiders-, luego el procesamiento de los mismos y, por último, su salid-outsiders-. Si revisamos el derogado tipo penal del fraude informático, veremos que únicamente contempla el procesamiento de datos y la salida de los mismos, dejando de lado su ingreso"*. De seguido el profesor Castillo realiza un comentario correcto, toda vez que, el artículo 217 bis siempre contempló el *"empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el procesamiento de datos del sistema"*, es decir, no estaba despenalizado ni excluido el ingreso de datos, en ese sentido indica Castillo: *"Esta afirmación de*

Tal y como se desprende, la Sala Tercera considera que *"influir en el procesamiento o resultado de los datos será manipular la información"*, es decir, aplica la regla de inferencia conocida como *modus ponens*, hace un razonamiento condicional, en el que si "p" entonces "q", "p" por lo tanto "q", es decir: *"si influye entonces manipula, influyó por lo tanto manipuló"*. Dicho razonamiento utilizado no es correcto, recordemos que se debe partir del concepto manipular en sentido estricto, por lo tanto, no todas las veces que se influye se manipula, se podría influir sin estar manipulando la información en un sentido estricto. Pero sí todas las veces que se manipula la información, se influye e incide en el sistema informático. La Sala Tercera iguala ambos verbos, cuando en realidad son distintos, contemplan supuestos diferentes.

Con la redacción actual del 217 bis del CP, tal y como lo refirió el profesor Castillo González, la manipulación solamente contempla el uso de datos falsos o incompletos, por lo tanto, se podría considerar que se está incidiendo en los datos del sistema; por otro lado, cuando los datos utilizados son verdaderos pero usados indebidamente, no se estaría alterando o incidiendo en el procesamiento de datos, tampoco se estaría manipulando el sistema en un sentido estricto, en virtud de lo anterior no lleva razón la Sala Tercera con esa afirmación. Se hace hincapié en lo siguiente: Si bien, esa interpretación hecha por Sala Tercera en el voto N° 148-2006, fue en cuanto a qué se debe entender por el verbo influir incorporado en el extinto delito de "fraude informático", lo cierto es que, reiteró ese criterio en la resolución N°1563-2014, es decir, dentro del periodo de estudio (ya vigente la estafa informática), circunstancia de interés puesto que, el delito de estafa informática mantuvo dentro de sus verbos "influir" y se le introdujo el de "manipular".

Chinchilla Sandí es discutible, pues el art. 217 bis Cód. pen. derogado decía, al definer (sic) la primera alternative (sic) de acción: "mediante programación o datos falsos o incompletos…", sin referir el empleo de programas o datos falsos a datos de entrada, a datos ya ingresados o a datos de salida." Es decir, el doctor Castillo, nos pretende dar a entender que, el articulado anterior, no distinguía en qué etapa del procesamiento de datos se debían emplear esos datos, por ende, incluía todas las posibilidades, incluso la fase de entrada. El razonamiento de Chinchilla era incorrecto porque entró a diferenciar en donde la ley no lo hacía.

Ahora bien, la citada resolución de Sala Tercera N° 2006-148, continúa indicando (aspectos no retomados en la resolución de la misma Sala N° 1563-2014): *"…Según indica el doctor Chinchilla Sandí, dentro de esas conductas destacan la* ***manipulación de los datos de entrada****: conocido también como sustracción de datos, es el más común en vista de la facilidad para la comisión y la dificultad en el descubrimiento. No requiere de conocimientos técnicos en informática y puede realizarlo cualquier persona que tenga acceso al procesamiento de datos en su fase de adquisición;* ***manipulación de programas****: difícil de descubrir pues el sujeto activo ha de tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en introducir nuevos programas o nuevas rutinas. Un método muy usado es el denominado "Caballo de Troya", el cual consiste en implantar instrucciones de computadora en forma subrepticia en un programa informático para que realice una función no autorizada al mismo tiempo que la normal;* ***manipulación de los datos de salida****: se lleva a cabo fijando un objetivo al funcionamiento del sistema informático, como el fraude a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos, lo que se hacía con tarjetas bancarias robadas. Ahora se usa equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y en las tarjetas de crédito..."*[306] De lo anterior se desprende cómo la Sala Tercera utiliza el concepto manipular en un sentido amplio, y lo aplica sin distinción en todas las fases de procesamiento de datos de un sistema informático.

La resolución de STCSJ N° 1563-2014, también hace un análisis concursal entre el delito de "fraude informático" y el delito de peculado: *"…"La defensa de los imputados alegó en sus conclusiones que la conducta de los imputados encuadra en el delito de Fraude Informático previsto en el numeral 217 Bis del Código Penal. Que como dicha norma no estaba vigente en el momento de los hechos, las acciones cometidas por los imputados eran atípicas. El Tribunal no comparte dicha apreciación. El artículo 217 Bis del Código Penal que contempla el delito de*

[306] El resaltado no corresponde al original.

*Fraude Informático, y que entró en vigencia el 24 de octubre de 2001, con posterioridad a estos hechos, dispone […] El Tribunal tiene claro que el medio por el cual se cometieron los delitos, lo fue un sistema informático, se utilizaron las computadoras de la Tesorería Nacional para a través del Sistema de Pagos TEF y posteriormente el de Créditos Directos, digitar los pagos ilícitos logrando sustraer el dinero mediante el desvío a cuentas clientes que no correspondían. Todo ello por medio del sistema SINPE que es un sistema informático […] La acción de sustraer como ya se expuso contiene cualquier forma de apoderamiento, entre ellas la utilización de medios informáticos. Es una norma que además de proteger el bien jurídico patrimonio, también protegido en el delito de Fraude Informático, protege un bien jurídico adicional, que es la probidad en el manejo de los bienes públicos de parte de los funcionarios encargados… **En el presente caso, precisamente los instrumentos informáticos fueron utilizados para influir en el procesamiento de datos** y lograr sustraer el dinero de la Tesorería Nacional, dinero que estaba bajo la percepción y administración de los imputados […] **El delito de fraude informático funciona como medio para cometer el delito fin, en este caso el Peculado**. El delito de Peculado puede cometerse de varias maneras, dentro de ellas por medios informáticos, ya que la norma no excluye dentro del concepto de sustracción, tal posibilidad. De allí que estamos ante un concurso aparente de normas, en el cual prevalece la norma especial que protege además del patrimonio, un bien jurídico adicional que no contiene el delito de Fraude Informático, que es la PROBIDAD en el ejercicio de la función pública. Además, la norma del 352 (sic) contiene integramente (sic) a la del 217 bis (si la consideraramos (sic) aplicable por favorecer al reo), por proteger el patrimonio, pero además tener otros elementos del tipo que son especializantes, que protegen la probidad, como lo es la calidad de funcionario público, la administración, percepción y custodia de los bienes públicos […] es adecuada la observación de los Jueces, al decir que la utilización del medio informático, en el caso particular, fue la manera para la sustracción de dineros públicos, y que su uso no genera por si solo la calificación que pretende el gestionante, toda vez que dicha acción está contenida íntegramente en el peculado, por lo que prevalece dicho tipo penal,*

acorde con las reglas del concurso aparente (art. 23 del Código Penal)…"[307] Ese mismo razonamiento fue utilizado por la Sala Tercera en la resolución N° 2018-00464 de las 16:25 horas del 20 de junio de 2018, en la que consideró que el delito de peculado y de fraude informático concurren aparentemente.

Por su parte, en la resolución Nº 2015-00354 de las 09:55 horas del 27 de febrero de 2015, la Sala Tercera por voto de mayoría consideró lícita la obtención de una clave o *password* de un programa informático sin autorización jurisdiccional, argumentando que no se vulneró el derecho a la privacidad o intimidad.

En la resolución Nº 2015-01292 de las 09:28 horas del 16 de octubre de 2015, la STCSJ, resolvió un conflicto de competencias por un delito de estafa informática, en el cual, el sujeto activo accedió al número de identificación y contraseña de la persona ofendida y de una empresa comercial, siendo que desde una dirección IP localizada en Lima, Perú, usó de manera indebida los datos obtenidos previamente, ingresó al sistema transaccional de Internet del Banco de Costa Rica, y trasladó dineros de la cuenta de la víctima a la de terceras personas. Determinó la STCSJ, que los actos de ejecución delictivos iniciaron desde una dirección electrónica fuera del país, pero los efectos o resultados se produjeron en suelo nacional, motivo por el cual, son aplicables los artículos 6 inciso 1) del CP y el inciso b) del artículo 47 del CPP, que asigna a la circunscripción judicial de la capital, el conocimiento de los delitos cometidos en el extranjero que producen sus efectos en el país.

En cuanto a las resoluciones anteriores al año 2014, provenientes de la STCSJ, en las pocas que existen, únicamente se trató la figura del fraude informático, por ejemplo: la resolución N° 2012-00032 de las 10:07 horas del 13 de enero de 2012, si bien, para ese momento no se había aprobado la reforma del 217 bis que cambió el tipo penal de fraude informático a estafa informática, la Sala Tercera consideró que dicho delito se pudiera cometer en coautoría, mencionó: *"…independientemente de quién fue la persona que manipuló a través de Internet*

[307] El resaltado no corresponde al original.

la cuenta bancaria del ofendido, la encartada P., tuvo la posibilidad de controlar la ejecución de ese hecho, al punto de que ella contribuyó no solo brindando la cuenta destinataria, sino también realizando el retiro del dinero, con lo que compartió el dominio funcional del hecho, por lo que validamente (sic) se comprueba su participación como autora del delito de fraude informático. Esta Sala ha indicado que el dominio funcional del hecho se establece a partir de la existencia del dolo común entre los partícipes, es decir, que todos asumen como un resultado propio el designado (elemento subjetivo), al igual que prestan una contribución al hecho (elemento objetivo), resultando responsables por la globalidad del actuar delictivo. Es irrelevante en qué estadio del iter criminis ha tenido lugar la actuación de cada uno de los sujetos involucrados. (Resolución 340-2007, de las 9:35 horas, del 13 de abril de 2007). El Tribunal con la certeza necesaria arribó a la conclusión de que la encartada participó en la actividad delictiva a título de autora, porque manipuló los datos del sistema e influyó en su procesamiento y obtuvo un beneficio patrimonial […] Observa esta Sala que para el Tribunal quedó demostrado el dominio funcional del hecho que mantuvo la encartada con sus colaboradores, porque ésta entregó la cuenta bancaria para hacer las transferencias de fondos y se presentó a realizar los retiros del dinero perteneciente al ofendido. Todo lo anterior evidenció gran precisión en la conducta ilícita de la encartada, dentro de una estructura delictual compleja, siendo ésta una persona más dentro de esa organización…"

Si bien, ese análisis de Sala Tercera no se realizó con respecto al delito de estafa informática, lo cierto es que, según la actual redacción del numeral 217 bis del CP, eso sí, siempre bajo un estudio casuístico, sí es posible la existencia de la coautoría en dicho delito informático, cuando se cumplan los siguientes requisitos[308]: **1)** Requisito objetivo: es decir que exista distribución de funciones sin la cual el hecho no se hubiera podido cometer, se debe realizar un ejercicio de supresión hipotética, eliminando el aporte y entonces nos preguntamos si el hecho

[308] Ver exposición de CALDERÓN CHINCHILLA, Rosaura. Seminario sobre Teoría del Delito. Colegio de Abogadas y Abogados de Costa Rica. En: https://youtu.be/I4pINwyHRU4, a partir del minutero 19:39.

subsiste o no, en caso de ser afirmativa la respuesta, entonces la persona no puede ser coautora, pero si la respuesta es negativa, sí puede serlo. **2)** Requisito subjetivo: es el plan previo, ponerse de acuerdo con otro para realizar el hecho, actos conclusivos para los sujetos activos. **3)** Requisito negativo: No puede tratarse de un delito de infracción a un deber, como lo son: delitos culposos, delitos de comisión por omisión, delitos de propia mano y delitos especiales propios.

De acuerdo a lo anterior, podría afirmarse que, la persona que dentro del plan previamente establecido facilita la cuenta bancaria como cuenta destino del dinero sustraído mediante un sistema informático, y la persona que se presenta a retirar el dinero sustraído en un cajero automático, realizan labores esenciales en el plan delictivo, sin las cuales el delito no se hubiera consumado. Y es que precisamente, la finalidad de los sujetos activos, en esa modalidad de comisión, es disponer en algún momento del dinero distraído, es decir, la intención no se agota en únicamente desviar el dinero de la cuenta bancaria del ofendido hacia otra cuenta bancaria, la finalidad está encaminada a obtener o procurar un beneficio patrimonial para sí o un tercero, tal como lo menciona el numeral 217 bis del CP, al final del primer párrafo: "…*con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro…"*

Además, en esa resolución N° 2012-0032, la Sala Tercera, en lo que respecta al verbo típico de la conducta, dispuso que se configuraba el delito de fraude informático tipificado en el artículo 217 bis del CP, básicamente el caso era el siguiente: el sujeto activo se impuso sin autorización del número de identificación (código de usuario) y de la contraseña bancaria de la persona ofendida, de modo tal que, desde una dirección IP, ingresó al sistema transaccional en Internet perteneciente a la entidad bancaria y utilizó indebidamente los datos, accedió al sistema y sin contar con autorización del titular de la cuenta, realizó una transacción bancaria, trasladando una cantidad de dinero a la cuenta de la persona imputada, quien ese mismo día, realizó retiros de dinero en una sucursal bancaria. La Sala señaló a la luz del caso en concreto e

interpretando la norma vigente para la época 217 bis del CP, fraude informático, en cuanto al verbo típico previsto en abstracto por el legislador: *"…Es así como,* ***la acción típica consiste, con el uso de medios informáticos para procesar información*** *que de alguna forma procure un beneficio económico al autor o a un tercero, mediante distracción de fondos, generación de errores contables, maquillaje de informes, entre otros. En la presente causa, se tiene que* ***la imputada con dominio funcional del hecho procedió a influir en el procesamiento*** *de datos de las cuentas bancarias del ofendido y* ***procedió a alterar el sistema*** *de tal manera que trasladó de la cuenta de la víctima A., a la suya la suma de un millón de colones […] El Tribunal con la certeza necesaria arribó a la conclusión de que la encartada participó en la actividad delictiva a título de autora,* ***porque manipuló los datos del sistema e influyó en su procesamiento y obtuvo un beneficio patrimonial*** *[…] Observa esta Cámara que las conclusiones a las que arribaron los juzgadores son el resultado de un proceso de análisis detallado de conformidad con las reglas de la sana crítica, que le permitió al Tribunal establecer que se cumple con los presupuestos enunciados en el numeral 217 del Código Penal (sic), en el tanto* ***se contó con la presencia de los verbos rectores, como procurar un beneficio patrimonial antijurídico, para la realización de obtención de dinero y además se procedió a influir en el procesamiento de datos, obteniendo información personal del ofendido, inmediatamente se hicieron los retiros, como parte de lo lógica delincuencial*** *(sic)."* [309]

Nótese como en esa resolución, de forma imprecisa, la Sala consideró inicialmente que el verbo típico era el *"uso de medios informáticos"* (esa afirmación es incorrecta a la luz de lo previsto en el artículo vigente para ese entonces), además, a la hora de analizar el caso concreto, la Sala resolvió de forma confusa, al considerar que el sujeto activo lo que hizo fue *"influir"* y *"alterar el sistema"*, circunstancias que en realidad son efectos de la acción humana de *"programación"*, *"empleo de datos falsos o incompletos"*, *"uso indebido de datos"*, o *"cualquier otra acción que incida"*. Recordemos que el tipo penal vigente para

[309] El resaltado no corresponde al original.

ese momento sancionaba a la persona "…*que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema"*. Asimismo, la Sala Tercera en ese voto mencionó: "*manipuló los datos del sistema e influyó en su procesamiento"*; de acuerdo con lo anterior, se evidencia una confusión en cuanto a lograr precisar cuál era el verbo activo del delito de "fraude informático".

De esa manera, se dejan expuestas las resoluciones más trascendentes emitidas por la STCSJ, sobre el delito de "estafa informática" y "fraude informático", durante el periodo de estudio.

Resoluciones del TASPIICJSJ del 2014 al 2019

De seguido se exponen los criterios jurisprudenciales del TASPIICJS, con respecto al tema de interés; realizadas las consultas en el sistema jurisprudencial "Nexus", con los parámetros de búsqueda *"estafa" "informática"* y *"217 bis"*, se obtuvieron los siguientes resultados:

Tabla 7. Resoluciones TASPIICJSJ sobre estafa informática del 2014 al 2019

Resoluciones emitidas por el TASPIICJS del 2014 al 2019 sobre el delito estafa informática (artículo 217 bis del CP)	
Año	**Cantidad de resoluciones**
2014 [310]	12

[310] Sean las siguientes resoluciones del TASPIICJS: **1)** 0521-2014 de las 11:00 horas del 19-03-2014; **2)** 600-2014 de las 13:22 horas del 28-03-2014; **3)** 1244-2014 de las 09:00 horas del 11-07-2014; **4)** 1413-2014 de las 10:20 horas del 05-08-2014; **5)** 1542-2014 de las 16:20 horas del 21-08-2014 (prórroga de medida cautelar); **6)** 1727-2014 de las 11:53 horas del 05-09-2014; **7)** 1732-2014 de las 14:32 horas del 05-09-2014; **8)** 2030-2014 de las 10:00 horas del 15-10-2014; **9)** 2037-2014 de las 14:07 horas 16-10-2014; **10)** 2097-2014 de las 15:45 horas del 23-10-2014; **11)** 2315-2014 de las 10:15 horas del 28-11-2014 (prórroga de medida cautelar); y **12)** 2433-2014 de las 15:10 horas del 17-12-2014 (prórroga de medida cautelar).

2015 [311]	10
2016 [312]	11
2017 [313]	4
2018 [314]	11
2019 [315]	3
Total	51

[311] Sean las siguientes resoluciones del TASPIICJS: **1)** 230-2015 a las 11:05 horas del 13-02-2015; **2)** 323-2015 a las 11:20 horas del 02-03-2015; **3)** 389-2015 de las 13:55 horas del 13-03-2015 (prórroga de medida cautelar); **4)** 436-2015 de las 09:10 horas del 20-03-2015; **5)** 535-2015 de las 17:45 horas del 09-04-2015 (prórroga de medida cautelar); **6)** 738-2015 de las 09:05 horas del 22-05-2015; **7)** 844-2015 de las 14:50 horas del 11-06-2015 (prórroga de medida cautelar); **8)** 917-2015 de las 15:20 horas del 25-06-2015 (el Sistema Jurisprudencial Nexus, arroja entre los resultados generales, con el parámetro de búsqueda "217 bis", una resolución con el número de voto "91-2015"; una vez consultado el enlace respectivo con ese número de resolución, se determina que el número correcto según fecha de la resolución y contenido, es "917-2015" y no "91-2015"); **9)** 1157-2015 de las 15:45 horas del 19-08-2015; y **10)** 1425-2015 de las 16:00 horas del 22-10-2015.

[312] Sean las siguientes resoluciones del TASPIICJS: **1)** 225-2016 de las 11:10 horas del 15-02-2016; **2)** 450-2016 de las 14:15 horas del 28-03-2016; **3)** 480-2016 de las 14:20 horas del 30-03-2016; **4)** 587-2016 de las 09:20 h del 22-04-2016; **5)** 690-2016 de las 15:30 h del 10-05-2016; **6)** 836-2016 de las 10:20 h del 06-06-2016; **7)** 976-2016 de las 15:05 h del 29-06-2016; **8)** 1326-2016 de las 13:40 h del 16-09-2016; **9)** 1496-2016 de las 15:15 h del 26-10-2016; **10)** 1700-2016 de las 10:35 h del 16-12-2016 (prórroga de medida cautelar); y **11)** 1768-2016 de las 15:00 h del 22-12-2016.

[313] Sean las siguientes resoluciones del TASPIICJS: **1)** 256-2017 de las 11:00 h del 03-03-2017; **2)** 617-2017 de las 14:20 h del 26-05-2017; **3)** 851-2017 de las 08:52 h del 12-07-2017; y **4)** 1016-2017 de las 10:45 h del 22-08-2017.

[314] Sean las siguientes resoluciones del TASPIICJS: **1)** 34-2018 de las 09:00 h del 17-01-2018; **2)** 197-2018 de las 09:30 h del 16-02-2018; **3)** 200-2018 al ser las 09:05 h del 16-02-2018; y **4)** 671-2018 de las 15:00 h del 28-05-2018 (prórroga de medida cautelar); **5)** 1048-2018 de las 09:55 h del 09-08-2018; **6)** 1082-2018 de las 10:25 h del 13-08-2018; **7)** 1280-2018 de las 10:35 h del 20-09-2018; **8)** 1643-2018 de las 11:25 h 19-11-2018; **9)** 1816-2018 de las 09:20 h del 13-12-2018; **10)** 1876-2018 de las 14:20 h del 18-12-2018 (prórroga de medida cautelar); y **11)** 1899-2018 de las 08:20 h del 21-12-2018.

[315] Sean las siguientes resoluciones del TASPIICJS: **1)** 97-2019 de las 15:20 h del 24-01-2019; **2)** 1431-2019 de las 16:10 h del 19-08-2019; y **3)** 1818-2019 de las 10:05 h del 11-10-2019.

En el voto N° 1244-2014 de las 09:00 horas del 11 de julio de 2014, el TASPIICJS, resolvió un asunto relacionado con el delito de fraude informático, indicando: *"…Cabe entonces determinar si se está en presencia de uno o nueve delitos de Fraude Informático en su modalidad de delito continuado. El artículo 217 bis del Código Penal, vigente para la fecha de los hechos (previo a la reforma de la Ley 9048 del 10 de julio de 2012), establecía el delito de Estafa Informática o Fraude Informático…"*[316] Nótese que el *ad quem*, trató ambos tipos penales como si fueran el mismo, circunstancia errada, en tanto el hecho de que uno precediera al otro en el mismo numeral del CP, no quiere decir que son iguales (precisamente por ello existió la reforma legislativa, que lo varió tanto en su título, como en su contenido), además, para evitar confusiones y procurar una mejor comprensión en las personas usuarias del sistema penal, se debe hacer un uso correcto del lenguaje tal cual está plasmado en la ley.

Más allá de ese error conceptual, el TASPIICJS consideró en ese caso concreto, el cual entró en su conocimiento mediante la fase de impugnación que, la siguiente conducta se subsume en el delito de "fraude informático": Varios sujetos actuando en coautoría, falsificaron tarjetas de crédito y débito que utilizaron para hacer compras en comercios; para ello, uno de los coimputados, que fungía como camarero en un restaurante, cobraba a los clientes y mediante la utilización de un *skimmer* (dispositivo informático en el cual se respalda la información almacenada en bandas magnéticas de tarjetas bancarias), creó una copia de la información contenida en las bandas magnéticas de tarjetas de pago originales de personas clientas atendidas por él; con los datos en su poder, almacenados en el dispositivo citado, los coencartados mediante la utilización de un equipo de cómputo y un software especial, reimprimieron la información sustraída en tarjetas tanto de crédito como débito, las cuales eran fabricadas por ellos y que personalizaron con el nombre de terceras personas, quienes fueron las que, posteriormente, se presentaron a los locales comerciales, adquirieron bienes o servicios que cancelaron con las tarjetas falsificadas, induciendo a error a los dependientes de los comercios ya que, sin percatarse de la falsedad de la tarjeta y

[316] Subrayado no corresponde al original.

creyendo que la persona que se encontraba en el establecimiento era el verdadero titular, le entregaron los productos solicitados, cuyos montos se cargaron a las cuentas de los verdaderos tarjeta habientes. Otro *modus operandi* fue que, mediante la falsedad de documentos, así como simulando ser empleados de un ente estatal, los mismos incriminados se presentaron a los locales comerciales, indujeron a error a los dependientes, quienes les vendieron mercadería.

En la resolución del Tribunal de Apelación no se analiza a fondo el tema de la tipicidad de las conductas, únicamente se limitan a considerar que se subsumen en el fraude informático, sin embargo, pareciera ser que, en los hechos en que medie un engaño hacia un dependiente, induciéndolo a error sobre quién era el verdadero titular de los datos usados en las compras, se pudo encuadrar la conducta en el delito de estafa general, tal cual se tratara de una estafa triangular. El profesor Francisco Castillo señala: *"Cuando una misma situación puede ser subsumida tanto en el art. 216 como en el art. 217 bis Cód. pen., el art. 217 bis retrocede frente al art. 216, pues aquél tiene el papel de ser un simple "Auffangtatbestand" (tipo penal de pezca (sic)), destinado a capturar los casos que no entran en el art. 216 Cód. pen. La estafa informática (art. 217 bis Cód. pen.) está en relación de exclusividad con relación a la estafa general (art. 216 Cód. pen.) Cuando la disminución patrimonial es consecuencia inmediata de una actuación errónea de un ser humano estamos frente a una estafa general del art. 216 Cód. pen. Por el contrario, cuando la disminución patrimonial es consecuencia inmediata del funcionamiento de un sistema de procesamiento de datos, entonces estamos en presencia de una estafa informática..."*[317]

Si bien, el razonamiento utilizado por el profesor Castillo es con respecto al concurso aparente entre estafa general y estafa informática, podría extrapolarse dicho análisis al caso resuelto por el TASPIICJSJ, toda vez que, parece extraerse un concurso aparente entre estafa general y fraude informático.

---

[317] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 135.

En la resolución N° 2014-0521 de las 11:00 horas del 19 de marzo de 2014 del TASPIICJS, se analizó un caso en el que, el sujeto activo del delito, una vez obtenidos los datos de la tarjeta de crédito mediante un "*skimmer"*, insertó la información en otro plástico con su nombre, y realizó una compra en un local comercial presentándole el documento falso al vendedor y a la cajera para el correspondiente pago. En esa ocasión, el TASPIICJS usó un léxico incorrecto, ya que erróneamente consideró que, el imputado había incurrido en el delito de estafa informática, ello a pesar de no ser de aplicación para el caso en concreto. Si bien, para cuando se emitió la resolución, el delito de estafa informática estaba vigente, lo cierto es que, el Tribunal de Juicio había condenado al imputado por delitos de fraude informático, a pesar de ello, el TASPIICJS haciendo eco de lo referido por el Tribunal Penal, indicó: "…*dichas identificaciones generan la certeza requerida para tener al acusado J como autor de dos Estafas Informáticas en concurso ideal llevadas a cabo el 27 de enero de 2005, ya que la información de la banda magnética usada en dicho momento no le pertenecía al acusado, siendo la misma alterada al igual que el plástico en el que se insertó para que coincidiera con los datos de identificación usados por el acusado en el documento de identidad que presentó al momento de la compra, como lo indicó la testigo A quien señaló en juicio que* ***"…También me presentó la cédula, y coincidía el nombre de la tarjeta con la cédula que me presentó…"***[318] En dicho asunto, nótese que sí existió un engaño, mediante el cual se indujo a error a la cajera, es decir, en principio se debió aplicar el delito de estafa general y no el fraude informático.

Llama la atención que, en dicha resolución, el TASPIICJS se limitó a transcribir la sentencia del Tribunal de Juicio, sin hacer un análisis sobre la figura penal de fraude informático, pero sí refrendó lo dicho por el *a quo*, de esa forma se deriva que, el *ad quem*, incurrió en un error al considerar que en el delito de fraude informático se induce a error al sistema informático, en tanto indicó dicho Tribunal de Apelación haciendo eco de la sentencia del Tribunal Penal: *"…Estos indicios y pruebas relacionadas entre sí no le dejan al Tribunal ninguna duda que el*

[318] El resaltado corresponde al original.

imputado J con pleno conocimiento, de que la tarjeta de crédito que va a utilizar en los comercios no le pertenece, que contiene datos falsos en la información, que el (sic) *introdujo y los cuales se pueden leer a simple vista, como el nombre de la persona, vencimiento, número de tarjeta, pero que contenía datos validos* (sic) *de otra persona, los cuales habían sido copiados fraudulentamente por él, en la banda magnética,* ***situación que hizo que se influyera en el normal procesamiento de los datos del sistema de computo*** (sic)***, por lo que una vez deslizada la tarjeta por el datafono*** (sic)*, se empieza a desarrollar una serie de procedimientos tecnológicos que tiene como objetivo, que el sistema autorice la compra que se está consultando,* ***provocando o llevando a error al sistema que en definitiva autoriza la compra****, las utiliza y con ello el imputado obtiene un beneficio patrimonial indebido con cada compra que realiza, en este caso de la Bomba Shell de San Rafael de Escazú, un beneficio total de cincuenta y tres mil seiscientos cuarenta y cinco colones…"*[319] Para poder encuadrar la conducta en una estafa general o en una estafa informática, es necesario demostrar o descartar la existencia de engaño que induzca a error, precisamente por esa razón, para los efectos de una investigación, es esencial conocer la dinámica en el momento preciso de la compra. ¿El sujeto activo realiza un movimiento corporal mediante el cual se identifica ante la persona dependiente? ¿Simula ser otra persona? ¿Oculta al cajero (persona física) que la información que contiene la tarjeta bancaria en la banda magnética no le pertenece? ¿Quién es la persona que desliza la tarjeta por el datáfono? ¿Cómo era el funcionamiento del datáfono, requería introducir la tarjeta, deslizarla o era de contacto? ¿Se engañó al cajero o a la cajera al momento de hacer el pago? En esas interrogantes radica el núcleo fundamental para derivar con precisión ante qué figura penal nos encontramos, siempre considerando las circunstancias del caso en concreto. *Prima facie*, podría pensarse que, si dentro de la dinámica del hecho, es el vendedor quien desliza en el datáfono la tarjeta que previamente le facilitó el sujeto activo, existiendo además, una identificación simultánea al pago o previa a este por parte del imputado, haciendo incurrir en error mediante un engaño al dependiente, ya que,

[319] El resaltado no corresponde al original.

no es la verdadera persona de la cédula o el verdadero titular de la información contenida en la banda magnética de la tarjeta utilizada, nos encontramos ante una estafa general. Pero cuando, del caso en concreto se pueda descartar la inducción a error al cajero humano mediante engaño o ardid, consecuentemente quedaría desplazada la estafa convencional, pudiendo ser considerada la estafa informática. Por ejemplo: cuando quien desliza la tarjeta en el datáfono es el mismo imputado, sin realizar previa identificación ante el cajero, sí podríamos estar ante el delito de estafa informática, sin embargo, será necesario indagar con la persona cajera, exactamente qué fue lo que ocurrió en el instante de la compra.

Vale resaltar que el TASPIICJS, indicó en la resolución que se viene estudiando: "…*El procedimiento para clonar la tarjeta según entiende este Tribunal es el siguiente: 1. Una persona de un local comercial tiene en su poder un Skimming de bolsillo, el cual se usa para leer y guardar la información que contienen las tarjetas de crédito y debido* (sic) *en las bandas magnéticas. 2. Luego el persona* (sic) *que trabaja en local comercial espera a que un cliente vaya a pagar con tarjeta y la pasa tanto por la maquina (sic) original de la tienda, llamada datafono* (sic) *y por su Skimming para guardar la información de la tarjeta, este procedimiento tarda pocos segundos. 3. Luego la persona que tiene el Skimming lo conecta a una computadora y pasa la información desde el Skimming hacia la computadora. 4. Posterior al proceso anterior, la persona utiliza una tarjeta en blanco con cinta magnética y la pasa por otra máquina llamada codificador de tarjetas de crédito para pasar la información de la computadora hacia la tarjeta en blanco. 5. A la tarjeta en blanco con la información verdadera se le introduce por medio de troquelado o letra Seth datos y fotografía de otra persona y así la tarjeta fraudulenta, o medio, o clonada, estará lista para usarse…"* Consideramos que si se cumplen a cabalidad cada uno de esos pasos, es posible afirmar que nos encontramos ante una estafa informática consumada, puesto que ya en ese momento los sujetos activos hicieron uso indebido de datos en un sistema automatizado de información y obtuvieron un beneficio indebido (adquirir los datos privados y sensibles de las víctimas).

En la resolución N° 600-2014 de las 13:22 horas del 28 de marzo de 2014 del TASPIICJS, si bien, no se analizó a fondo la aplicación del delito de fraude informático, sí indicó el *ad quem*, que la siguiente conducta se subsume en ese ilícito penal: Unos sujetos actúan en coautoría, ellos se dedicaron a copiar y alterar los datos de sistemas informáticos de distintas empresas emisoras de tarjetas de crédito, una vez con los datos en su poder, por medio de la utilización de las denominadas "tarjetas medio", hicieron compras en locales comerciales actuando en contubernio con los dependientes y administradores de esos locales, percibiendo ilícitamente beneficios económicos antijurídicos en perjuicio de diferentes tarjeta-habientes y de las mismas entidades bancarias emisoras de las tarjetas. En este caso, sí es claro que no existió un engaño a una persona, razón por la cual se descarta el delito de estafa general y sí resulta de aplicación el antiguo fraude informático por el uso indebido de datos, ya que influyeron en el procesamiento de los datos de un sistema informático.

En la resolución N° 1732-2014 de las 14:32 horas del 05 de septiembre de 2014, el TASPIICJS, subsumió la siguiente conducta en el delito de hurto simple, descartó aplicar el delito de "fraude informático" (acusado por el Ministerio Público), y omitió hacer referencia al delito de estafa general: El sujeto activo por la confianza que tenía con el ofendido, se impuso de su número de identificación (código de usuario) así como de su contraseña, accedió a la cuenta bancaria y en diecisiete ocasiones distintas le sustrajo dinero. Señaló el Tribunal de Apelación: "…*el imputado urdió un plan que le permitiría de manera ilícita sustraer ese dinero, y* ***mantener al ofendido en error****, el cual consistió en ayudarle a crear un usuario en internet banking, acompañarlo a solicitar el dispositivo HWToken al Banco Nacional e indicarle que realizaría compras vía internet para su beneficio […] Contrario a ello, con los datos electrónicos en su poder sustrajo el dinero del ofendido para su propio beneficio y sin mediar autorización de la víctima para tales fines. Por otra parte, el Tribunal tuvo como hechos probados que el imputado logró obtener de parte del ofendido el número de identificación y la contraseña de acceso a la cuenta bancaria de éste y creo* (sic) *un plan para imponerse de manera ilegítima del dinero propiedad de la víctima […] y* ***lo mantuvo en error***

bajo la falsa creencia que le ayudaría inicialmente a crear el usuario en internet banking*, lo acompañó a solicitar el dispositivo HWToken y le indicó que realizaría compras para beneficio del ofendido cuando en realidad, la finalidad del encausado era obtener esos datos para acceder al sistema banking e influir en el procesamiento de éste mediante el uso indebido de datos, lograr el traslado ilícito hacia sus cuentas y obtener un beneficio patrimonial antijurídico […] de las pruebas evacuadas y analizadas por parte del a quo, el imputado sí obtuvo los datos de internet banking y el HWToken de parte del ofendido, lo que resulta ilegítimo y así lo tuvo por demostrado el Tribunal fue el uso que le dio el encartado a dicha información, porque en ningún momento fue para beneficio del ofendido […] Por lo que no queda duda, que efectivamente el imputado se aprovechó de la confianza que le tenía su familiar al facilitarle el token y todos los datos bancarios para sustraer el dinero poco a poco de la cuenta del ofendido.* ***Así lo pudo engañar indicándole que iba a comprar bienes por internet que serían para él, como un teléfono, un torno, una computadora, bienes que nunca le fueron entregados*** *[…] de ahí, que ante la voluntariedad del ofendido de dar sus datos bancarios, este acto, se podría asimilar como si hubiese dejado ingresar al imputado a su vivienda y éste hubiera sustraído la computadora o un teléfono de la casa de habitación de la víctima. Por ello, no encuentra defecto esta Cámara en la calificación dada a los hechos,* ***por que sí existió engaño****, el cual lo mantuvo hasta que el ofendido se enteró del faltante de dinero en su cuenta, obtuvo los datos de manera lícita, pero hizo uso de ellos de forma ilegítima…"*[320]

De acuerdo a los razonamientos externados por el Tribunal *ad quem*, sí existió un engaño mediante el cual se indujo a error al ofendido, sin embargo, no se hace mención del por qué se descartó la estafa general. Si consideramos tanto el nombre de usuario y la clave secreta como parte del patrimonio de la víctima, estaríamos ante una estafa convencional, sin embargo, ello sería incurrir en una interpretación analógica *in malam partem*. El hecho de que se indujera en error a una persona física en el caso en concreto, ameritaba realizar un análisis referente a los elementos objetivos del tipo penal 216 del Código Penal.

[320] El resaltado no corresponde al original.

Ahora bien, el TASPIICJS, haciendo eco de la resolución del Tribunal *a quo*, consideró que no era de aplicación el fraude informático por la siguiente razón: "…*Estamos en presencia de diversas conductas típicas, antijurídicas y culpables cometidas por el encartado, las que sin embargo no configuran diecisiete delitos de Fraude Informático como se han venido imputando, siendo que en su lugar se realizaron diecisiete delitos de Hurto Simple. Para ello ha estimado el Tribunal que no concurren los presupuestos objetivos del tipo penal de Fraude Informático establecido en el numeral 217 bis del Código Penal para la fecha de las conductas acusadas, pues se ha considerado que dadas las circunstancias no se influyó o incidió en el procesamiento de datos, pues el encartado empleó los datos verdaderos del legítimo cuentacorrentista, sea sus datos de identificación, su contraseña y posiblemente su token en las condiciones irregulares que ya se han enunciado y según el marco de confianza que se ganó el acusado, ya detallado. Cuando se habla de influir o incidir, el verbo se refiere al verbo "manipular", pues es preciso determinar los alcances de estas acciones a fin de determinar si se está de cara ante la conducta de un Fraude Informático. Según el Diccionario de la Real Academia de la Lengua Española, la manipulación consiste en la acción y efecto de manipular, esto es, en una primera acepción, "operar con las manos o con cualquier instrumento"; pero en una segunda acepción, que es la que nos interesa, en "intervenir con medios hábiles y a vez arteros (mañosos, astutos, en mal sentido) en la política, en la sociedad, en el mercado, etc., con frecuencia para servir a los intereses propios o ajenos. Por manipulación, desde el punto de vista jurídico, se entiende cualquier acción voluntaria de intervenir o afectar, de forma subrepticia, inautorizada y astuta, elementos o bienes tangibles o intangibles, afectando intereses objeto de protección jurídico penal (Ver CHINCHILLA SANDÍ, Carlos, Delitos Informáticos, Farben 2004, p. 267). De acuerdo con Cándido Conde, el concepto de manipulación informática significa una alteración o modificación de los presupuestos básicos del sistema o de las órdenes recibidas por éste, de modo que produzca resultados no previstos o que no habría autorizado, de conocerlos, el instalador o titular del sistema o el titular de los datos y valores económicos*

procesados por el sistema. El concepto de manipulación informática se corresponde con la conducta de alterar, modificar u ocultar datos informáticos de manera que, se realicen operaciones de forma incorrecta o que no se lleven a cabo, y también con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener. El concepto de manipulación informática se corresponde con la conducta de alterar, modificar u ocultar datos informáticos de manera que se realicen operaciones de forma incorrecta o que no se lleven a cabo, y también con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener. Sin embargo aquí se ha tenido por demostrado que el encartado luego de que el imputado se ganara su confianza, se impuso de la información necesaria que todo cliente legítimo ocupa para acceder a su cuenta personal, con lo cual se apartan los verbos de influir, incidir o manipular a que se refiere la acción delictiva del Fraude Informático. En su lugar, estima el Tribunal que se configuran 17 delitos de Hurto Simple, descrito en el numeral 208 del Código Penal […] En el considerando primero de este voto, se transcriben las circunstancias que tomó en cuenta el Tribunal para realizar la recalificación a hurto simple y se estableció que la calificación es acorde con los hechos acusados y demostrados en debate, analizando asimismo, que, ***aunque se hable de ardid y engaño, utilizados por el encartado para sustraer el dinero del ofendido de su cuenta bancaria, no precisamente debe calificarse como fraude informático****, debido a que el imputado tuvo acceso a las cuentas de banco de la víctima por qué ella misma le facilitó los datos necesarios para ingresar a dichas cuentas, no existió manipulación a nivel electrónico o digital de parte del encartado para lograr su cometido…"*[321]

El razonamiento utilizado tiene varias falencias, entre ellas: **1)** El uso indebido de datos, si bien, no se debe entender como una manipulación del sistema informático, lo cierto es que, sí influye en el procesamiento de datos. **2)** Confunde el significado de los verbos infinitivos: influir, incidir y manipular. **3)** El ardid o engaño no es un elemento objetivo del tipo penal de fraude informático ni

[321] El subrayado y resaltado no corresponden al original.

de la actual estafa informática, razón por la cual, la ausencia de esos elementos no descarta la subsunción de la conducta en alguno de ellos. En todo caso, resulta cuestionable encajar dicho comportamiento en el delito de hurto simple, puesto que la finalidad del autor fue usar indebidamente los datos mediante transacciones bancarias, circunstancia que aleja la conducta del delito de hurto. De igual manera, las sustracciones de dinero se materializaron por el procesamiento de datos, es decir, los computadores utilizados, simplemente obedecieron las instrucciones o comandos que el imputado les ingresó, siendo que, existió una influencia en el sistema automatizado de procesamiento de datos mediante la modalidad de datos indebidos, conducta que sí estaba sancionada en el ordenamiento jurídico al momento de los hechos, circunstancia que se corrobora mediante la siguiente resolución del TASPIICJSJ, la cual comparto:

En el voto N.º 450-2016 de las 14:15 horas del 28 de marzo de 2016 del TASPIICJSJ, se analizó un asunto en el que el sujeto activo, conociendo la clave de la cuenta bancaria de la ofendida, telefónicamente realizó transacciones bancarias hacia su cuenta, y posteriormente, en un cajero automático realizó los retiros correspondientes, el *a quo*, lo condenó por delitos de hurto agravado en la modalidad de delito continuado, por su parte el *ad quem*, consideró que la figura aplicable al caso en concreto era la estafa informática. En dicha resolución, se analizan criterios dictados por la Sala Tercera, relacionados con el tema, en lo que interesa el Tribunal de Apelación mencionó: *"…Tratándose del fraude informático, también denominado estafa informática (art. 217 bis del Código Penal), lo primero que hay que señalar es que a pesar de su nombre, en este tipo penal no se contempla una estafa en sentido estricto, pues el sujeto activo no engaña a otro para que este, inducido a error, tome una disposición patrimonial perjudicial, para sí, o para un tercero. Lo que se prevé es únicamente la ejecución de un fraude que permite la obtención del beneficio patrimonial antijurídico. Pese a que, es de suponer, el legislador pretendía prohibir la conducta de los denominados hackers que ingresan en los sistemas informáticos de manera irregular para apropiarse del patrimonio ajeno, el tipo penal se formuló de manera mucho más amplia. Según se extrae de su lectura, la conducta prohibida es*

manipular o influir en el ingreso, en el procesamiento o en el resultado de los datos del sistema automatizado de información a través de los siguientes mecanismos: 1) usar datos falsos o incompletos; 2) usar indebidamente datos; 3) programar, 4) ejecutar alguna operación informática o usar artificio tecnológico alguno o, 5) realizar cualquier otra acción que incida en el procesamiento de los datos del sistema o dé como resultado información falsa, incompleta o fraudulenta. Lo esencial en este tipo penal, por tanto, es la manipulación o influencia que se ejerce sobre un sistema automatizado de información (aquí es donde radica el timo), con el propósito de conseguir una transferencia de activos no autorizada por el titular […] Como se observa, la jurisprudencia se ha dado a la tarea de establecer algunos parámetros para aplicar el tipo penal de la estafa informática, algunos de los cuales si bien esta integración respeta, no comparte por lo que de seguido se expondrá. Tenemos que, en este asunto, se imputó y se tuvo por demostrado que (…) el 4 de enero de 2013, con conocimiento de la clave de acceso o PIN de una de las cuentas de la víctima en el Banco de Costa Rica, influyó en el sistema desde el número de teléfono (…) y sin autorización alguna, transfirió de esa a la suya, una suma de ₡500.000 colones, dinero que retiró en un cajero automático. Posteriormente, el 7 de enero transfirió ₡200.000 y el 8 de enero transfirió ₡30.000 colones, sumas que retiró en un cajero automático (folios 59 y 60, 109 a 111 frente). Como se extrae de este cuadro fáctico, la imputada, con el propósito de obtener un beneficio patrimonial indebido para sí (elemento subjetivo distinto al dolo que prevé el tipo penal de la estafa informática), usó indebidamente la clave o PIN de [Nombre 001] para ingresar al sistema y trasladar fondos de las cuentas de este a la suya, en cantidades que también la misma imputada definió. A través de esta conducta, que (…) realizó en tres ocasiones valiéndose de la plataforma tecnológica suministrada por el banco (entiéndase, Bancatel), influyó en el ingreso de los datos del sistema automatizado, causándole un perjuicio económico al agraviado, lo que resulta suficiente para concluir que se configuró el delito previsto en el numeral 217 bis del Código Penal. Para este tribunal, no se requiere que el sujeto activo posea destrezas particulares, o una posición estratégica que le permita manipular o influir en el sistema haciendo "algo distinto" a lo que hubiese

hecho el propio titular de la cuenta, como lo argumenta el a quo con base en lo expuesto por la Sala Tercera de la Corte Suprema de Justicia, lo anterior en tanto que el tipo penal no prevé ese requerimiento. En este, se insiste, se prohíbe manipular o influir en el ingreso, en el procesamiento, o en el resultado de los datos de un sistema automatizado de información por alguno de los mecanismos ya descritos y si bien la manipulación, según el Diccionario de la Lengua Española, en una de sus acepciones, significa "Intervenir con medios hábiles y a veces arteros, en la política, en el mercado, en la información, etc., con distorsión de la verdad o la justicia, y al servicio de intereses particulares", ***se tiene que el legislador también contempló el verbo influir, que para este tribunal, no es sinónimo del anterior****. En ese sentido, la Real Academia Española sostiene en cuanto a este, que dicho de una cosa significa "producir sobre otra ciertos efectos", siendo justamente lo que sucedió cuando la imputada, haciendo un uso indebido de los datos de la víctima, los ingresó al sistema para hacer las transferencias. Dicho en otras palabras, influyó en el ingreso de los datos de un sistema automatizado (Bancatel) mediante el uso indebido de los datos de la víctima. La cláusula contenida en el tipo penal resulta lo suficientemente abierta para comprender conductas como la descrita en la imputación formulada por el órgano requirente, dirigida a conseguir una transferencia de fondos no consentida por el titular, con lo cual no es indispensable que el sujeto activo tenga conocimientos o destrezas particulares que le permitan hacer lo que otros, de ordinario, no pueden efectuar. Finalmente, también se debe subrayar que el tipo penal no solo contempla el uso de datos falsos o incompletos, sino también el uso indebido de datos, supuesto que se articula en este asunto, pues si bien la clave o PIN es la auténtica, la víctima nunca suministró a (…) esa información y menos aun consintió su empleo…"*[322]

En ese mismo sentido, de forma correcta, el TASPIICJSJ en la resolución N° 1082-2018 de las 10:25 horas del 13 de agosto de 2018, sí consideró que el uso indebido de datos, influye en el sistema informático, refirió el *ad quem*: *"…El tribunal de mérito analizó que la acción atribuida al imputado (…) consistió en que,*

[322] El resaltado y subrayado no corresponde al original.

en asocio con personas desconocidas, tuvo acceso a los datos de usuario y contraseña pertenecientes a ambos ofendidos, los que eran necesarios para ingresar al sistema "en línea" del Banco de Costa Rica. Apunta cómo se evidenció la existencia de un plan y el acuerdo previo, atendiendo a la sincronización de las acciones, pues las transacciones se hicieron desde una dirección IP en Perú y el encausado procedió a realizar, ese mismo día, los retiros en pocas horas […] Es así que las juzgadoras no se limitaron a señalar que el dinero trasladado de las cuentas de los ofendidos fue a dar a las cuentas en colones y en dólares del encausado (…), sino que expresaron una serie de elementos probatorios que llevaron al juicio de certeza de que en contubernio con sujetos desconocidos, influyó en el sistema "en línea" del Banco de Costa Rica, y mediante el uso indebido de los datos de las víctimas (usuario y contraseña), lograron transferir fondos a sus cuentas personales..."

En el voto N° 738-2015 de las 09:05 horas del 22 de mayo de 2015, el TASPIICJSJ, realizó la siguiente acotación con respecto a los delitos de hurto y fraude informático, ello en un asunto en el que el sujeto activo utilizó indebidamente los datos del ofendido (número de cuenta bancaria y clave de acceso) en el portal de Internet de una entidad bancaria y realizó transferencias de dinero: *"…es importante tener presente que, aunque hubiese un apoderamiento ilegítimo, o un beneficio patrimonial indebido, la figura del hurto simple, sería de carácter general, respecto de la del fraude informático, que tiene varios componentes especializantes, como lo son, que debe cometerse utilizando un sistema de cómputo; por medio de la manipulación de la información que esté codificada, o sistematizada en aquel; y bajo un determinado programa de informática. Precisamente, estos tipos penales que podrían decirse "novedosos" responden a la necesidad de proteger una serie de actividades propias de esta era, caracterizada por el uso de la herramienta del internet, que facilita una gran cantidad de actividades económicas en el mundo. De modo que la figura del hurto simple, se ve desplazada, cuando se presentan estos otros elementos especiales que pueden tener la misma característica, de permitir un beneficio económico indebido, solo que se comete por medio del uso de una computadora y un sistema*

informático…" A nuestro criterio, tal y como se ha venido exponiendo en el desarrollo de la investigación, cuando exista un uso indebido de datos en un sistema automatizado de información mediante el cual se influya en el procesamiento de datos y se obtenga un beneficio patrimonial, no es posible subsumir esa conducta en el delito de hurto, por lo tanto, no concurre ni siquiera aparentemente con la estafa informática, razón por la cual no se comparte lo indicado por el Tribunal de Apelación en la *supra* citada resolución, la cual incurre en otro yerro al momento de interpretar el verbo "manipular".

De acuerdo con dicho análisis, cabe preguntarse: ¿Concurre aparentemente el delito de hurto en la conducta desplegada por el sujeto activo de usar indebidamente datos en un cajero automático, obteniendo dinero en efectivo? Para aclarar dicho entuerto, podemos remitirnos a la siguiente nota, la cual comparto y rescato para el caso costarricense: *"Al menos en lo que respecta al hurto, el Tribunal Supremo Federal alemán zanjó la discusión mediante su fallo de 16 de diciembre de 1987 (BGHSt 35, 152), conforme al cual la conducta no es subsumible a título de hurto porque no constituye "sustracción" en los términos del § 242 StGB, ya que el agente no arrebata la custodia de la cosa sino que la recibe del cajero automático de acuerdo con la programación establecida por el responsable del mismo, siendo indiferente que quien usara la tarjeta y la clave no estuviera legitimado para ello. Para el tribunal resulta decisiva la apariencia externa del proceso de obtención del dinero, y en este caso tal apariencia es la de una verdadera entrega hecha por el titular del dinero a través del cajero automático. La situación sería idéntica a la que se da cuando un subordinado recibe el encargo de entregar una determinada cantidad de dinero a quien se presente con una tarjeta determinada y dé un número secreto correcto. En este caso, si se presenta alguien no autorizado que, sin embargo, cumple con tales requisitos y recibe el dinero, no podría negarse que hubo a su respecto una disposición patrimonial que excluye conceptualmente la sustracción (BGHSt 35,*

152 [158 y s.])…"[323] En el delito de hurto, lo que existe es un apoderamiento de la cosa por parte del agente sin participación alguna de la víctima (sujeto activo alarga la mano y se apodera de la cosa ajena)[324], circunstancia que por ejemplo, no se presenta en los retiros de dinero en cajeros automáticos mediante el uso indebido de datos, en los cuales sí hay una participación de la víctima, tal y como se expondrá de seguido:

El tema se encuentra directamente relacionado con quién es la víctima en dichas situaciones: *"Pues bien, el problema de la aplicación del tipo penal de hurto en estos casos es que la figura, en cuanto delito contra la propiedad, sólo sirve a la protección del dueño de las cosas corporales muebles apropiadas, es decir, al dueño de los billetes que se encuentran en el cajero automático y no a la del titular del patrimonio perjudicado con ello. En otras palabras, contra toda intuición y evidencia en cuanto a los verdaderos intereses en juego, la víctima del delito es el operador del cajero automático, por regla general el banco, y no el titular de la tarjeta. Desde un punto de vista procesal, el titular de la tarjeta no debería ser admitido como víctima en el procedimiento […] de modo que no debería poder querellarse, ni celebrar acuerdos reparatorios ni obtener reparación civil en sede criminal. Y si bien nuestros tribunales nunca han sido especialmente rigurosos en la aplicación de estas normas, lo que unido a la pasividad que en general exhiben los bancos en estos casos permite que a menudo el titular de la tarjeta de hecho intervenga en calidad de víctima, en el evento de disputa entre éste y el banco debería resolverse inequívocamente en favor del último."*[325]

---

[323] HERNÁNDEZ BASUALDO, Héctor. *Uso indebido de tarjetas falsificadas o sustraídas y de sus claves*. En Revista Electrónica Política Criminal, Nº 5, A2-5. Chile, 2008, pp. 8-9. Versión digital en: http://politcrim.com/wp-content/uploads/2019/04/A_2_5.pdf.

[324] SÁNCHEZ DELGADO, Daniel. *La estafa. Análisis de sus elementos y problemática con los llamados delitos informáticos*. En: Revista Judicial. Tomo I. Año XX. N° 65, San José, 1997, p. 55.

[325] HERNÁNDEZ BASUALDO, Héctor. *Uso indebido de tarjetas falsificadas o sustraídas y de sus claves*. . En Revista Electrónica Política Criminal, Nº 5, A2-5, Chile, 2008. p. 14. Versión digital en: http://politcrim.com/wp-content/uploads/2019/04/A_2_5.pdf. Ver en ese mismo sentido: CALDERÓN CAMPOS, Marta Eunice. *Marco jurídico de la profesión informática en Costa Rica*. Editorial Universidad de Costa Rica (UCR), Costa Rica, 1ª ed. 2018, pp. 66-70: *"El artículo 35 de la Ley 7472 de la Promoción de la Competencia y Defensa Efectiva del Consumidor establece la*

En ese mismo sentido, la resolución N° 851-2017 de las 08:52 horas del 12 de julio de 2017, el TASPIICJSJ, relacionado con quién es el ofendido en los delitos de estafa informática cuando se trata de uso de tarjetas bancarias de una forma indebida, mencionó: *"…Se alegó que los ofendidos no fueron traídos a declarar durante el debate, lo que se consideró considerados* (sic) *como los propietarios de las cuentas bancarias de las cuáles se extrajeron los montos. Siendo que resultaba irrelevante el determinar si cada uno de ellos estaba de acuerdo con las transacciones realizadas. Sin embargo, se deja de la* (sic) *lado por los recurrentes que los hechos denunciados son de acción pública y que, por lo tanto, son perseguibles por el Estado, sin requerir el accionar del perjudicado directo.* ***En éste tipo de defraudaciones no se puede considerar como ofendido únicamente a los titulares reales de las tarjetas de crédito, ya que en muchos casos el perjudicado directo, al final puede ser la empresa aseguradora****, ya que la mayoría de las entidades bancarias o financieras, resguardan sus operaciones financieras adquiriendo seguros para proteger sus inversiones. En éste caso,* ***hay una pluralidad de afectados, a saber las empresas comerciales donde fueron utilizadas las tarjetas de crédito falsas, las empresas propietarias de las máquinas lectoras de las tarjetas de crédito***

---

responsabilidad de productores, proveedores y comerciantes cuando el consumidor resulta afectado por el uso de los bienes o servicios que aquellos le brinda; una entidad bancaria es un proveedor de servicios y, por tanto, está sujeto a esta ley". De igual manera, la autora hace alusión a la resolución N° 300-F-S1-2009 de la Sala Primera de la Corte Suprema de Justicia del 26 de marzo de 2009: *"En el mismo sentido, luego de analizado el testimonio en comentario, quedó demostrado que la plataforma informática del Banco (…) no fue vulnerada para obtener la clave y el usuario de la señora (…), aspecto sobre el cual lleva razón el recurrente, y que la seguridad con que cuenta resulta adecuada para proteger la integridad de la base de datos y la plataforma transaccional a lo interno. No obstante lo anterior, debe tomar en cuenta la entidad financiera demandada que su función esencial es la intermediación financiera, que incluye la captación de fondos provenientes del ahorro del público, concepto que lleva implícita su custodia, tanto desde el punto de vista físico, como del registro electrónico correspondiente. No cabe duda que se encuentra sometida a una ineludible obligación de garantizar la seguridad de las transacciones realizadas, ya sea en ventanilla o mediante cualquier otro medio puesto a disposición de los clientes, la cual debe abarcar, necesariamente, el uso de todos aquellos mecanismos disponibles que le permitan contar con un mayor grado de certeza en cuanto a la identificación de las personas que se encuentran facultadas para realizar transacciones electrónicas desde las cuentas. La responsabilidad que le fue imputada al Banco se fundamenta, no en la sustracción del dinero por un tercero, sino en la existencia de un riesgo, según lo expuesto en el considerando III, en el funcionamiento propio del servicio que ofrece, lo que permite imputar el origen del daño al funcionamiento del servicio […] Lo anterior, a pesar de disponer de mecanismos que permiten mayor seguridad."*

(en éste caso Credomatic), las empresas emisoras de las tarjetas de créditos, así como los adquirentes de las tarjetas de crédito a quienes les copiaron la información, y las aseguradoras que cubrieron los pagos producto de las compras fraudulentas*. Ahora bien, independientemente de esa situación, basta con tener claro que los propietarios de las tarjetas de crédito "originales o verdaderas" no ingresaron no estuvieron nunca en los locales comerciales en las que las tarjetas de crédito duplicadas, fueron utilizadas, sin que se requiera la presencia de los mismos en debate. A efectos de acreditar el perjuicio en éste asunto la afectación se verificó desde el momento en que se realizaron acciones que vulneraron la seguridad del sistema lector de las tarjetas de crédito y se aprobó una transacción que fue realizada con datos "clonados" y que no pertenecían al emisor de la tarjeta de crédito original.* ***No es cierto que la empresa financiera Credomatic, no es una empresa ofendida, ya que fueron sus máquinas lectoras de la información inserta de las tarjetas de crédito, las que fueron vulneradas, y son responsables ante las personas dueñas de las cuentas a las que correspondían las tarjetas de crédito originales****. De forma que, desde el momento en que, ante la utilización de plásticos con información clonada, se vulnera los sistemas lectores de los datos informáticos, se generó la afectación…"*[326]

Si bien el numeral 208 del CP costarricense, denominado "Hurto", no contiene el verbo "sustraer", sí tipifica el verbo "apoderarse ilegítimamente", sin embargo, el hecho que sea el cajero automático el aparato que dispensa el dinero obedeciendo las instrucciones, involucra una variante que se torna en nuclear, y es que, el sujeto activo, la conducta que lleva a cabo, es ingresar datos mediante un teclado, por lo que la computadora procesa los mismos, por tanto, es la entidad bancaria encargada del resguardo del dinero, la que por medio del cajero automático, le facilita el dinero al agente, quien previamente ingresó los datos

[326] Dicho criterio, encuentra respaldo inclusive en la doctrina costarricense, el doctor Francisco Castillo, señala con respecto al uso indebido de datos en el delito de estafa informática: *"Creemos que el sujeto titular del bien jurídico es aquel que tiene un derecho inmediato a trabajar, a borrar o a utilizar los datos."* CASTILLO GONZÁLEZ, Francisco. *La estafa informática de "Lege lata" y de "lege ferenda"*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., p. 287.

idóneos para que informáticamente se procesaran y obtener un resultado. Precisamente, es fundamental conocer cómo entra en poder de la cosa el sujeto activo, ya que, si prescindiéramos de esa circunstancia, y únicamente contempláramos el verbo “apoderar” en sentido amplio, la mayoría de delitos contra la propiedad constituirían un hurto, lo cual no es correcto, ya que existen diversas maneras de apoderarse de un bien, como por ejemplo el delito del numeral 223 del CP, denominado “Apropiación y retención indebidas”. De acuerdo con lo anterior y por la dinámica del hecho, es posible excluir el delito de hurto en el caso analizado.

Es importante hacer referencia que el TASPIICJ en el citado voto N° 738-2015, realizó una acotación trascendente: *“De manera que hubo un abuso de confianza que, a su vez, implicó que se diera un* ***uso indebido*** *de esos datos, en esa medida, es que debe entenderse que el acusado* ***influyó en el resultado de los datos del sistema de cómputo*** *al trasladar, por medios electrónicos, el dinero de una cuenta a otra, cuando no le pertenecía ni tenía autorización de su dueño para hacerlo…”* Claramente interpretó el Tribunal, que el hecho de usar datos verdaderos implica que se influye en el sistema informático, siendo hasta en esta resolución, que jurisprudencialmente se interpretó dicha situación. A pesar de ello, el *ad quem*, en el mismo voto agregó: *“…influir o incidir son acciones que se refieren a la manipulación del sistema y, desde el punto de vista jurídico, se entiende que es cualquier acción voluntaria que interviene, o afecta, de manera inautorizada, la protección que brinda el sistema informático, en este caso, bancario, para las cuentas electrónicas de sus legítimos usuarios…”* Es importante hacer hincapié, en que ese análisis fue realizado en aplicación de la figura de fraude informático y no propiamente de la estafa informática, pero debe tomarse en cuenta, debido a la interpretación que desde ese entonces se le ha dado al verbo manipular, el cual, según lo hemos analizado en el presente trabajo, se presenta cuando estamos ante uso de datos falsos o incompletos, en los cuales sí se incide mediante manipulación. A pesar de ello, atendiendo nuestro numeral 217 bis del CP, se hace innecesario recurrir al verbo manipular, ante la influencia en el sistema por medio de la acción del uso de datos.

En la resolución N° 436-2015 de las 09:10 horas del 20 de marzo de 2015, el TASPIICJSJ confirmó una sentencia condenatoria por los delitos de estafas informáticas, cometidos en coautoría, siendo que los sujetos activos usaron indebidamente datos que estaban almacenados en tarjetas falsas, las cuales insertaron en cajeros automáticos, retirando dinero de manera ilegítima, afectando una entidad bancaria estatal. En ese sentido, mencionó el Tribunal *ad quem*, al responder uno de los motivos de impugnación presentados por la defensa técnica de los sentenciados: *"…**que es precisamente una de las modalidades que puede asumir el delito de "Estafa informática" cuando se realiza mediante el uso indebido de datos, para manipular fraudulentamente el procesamiento de un sistema automatizado de información, como el de los cajeros automáticos**, para procurar u obtener un beneficio patrimonial indebido para sí o para otro […] Lo que sí se acreditó es que, mediante el uso indebido de las tarjetas falsas o "clonadas" que tenían en su poder, los cuatro imputados procuraron y obtuvieron indebidamente dinero en efectivo de los cajeros del Banco de Costa Rica…"*[327] Si bien, subsumió correctamente la conducta en el tipo penal, los razonamientos utilizados no son del todo válidos, ya que tal y como se mencionó párrafos atrás, el uso indebido de datos no implica una manipulación del sistema automatizado, lo que sí se produce como consecuencia del uso indebido de datos, es influir en el sistema informático para que procese la información y consecuentemente influir en el resultado, en este caso, el cajero automático al recibir los datos correctos, simplemente los procesó, al validar una orden consecuente con su programación obedeció las instrucciones y facilitó el dinero. En ese sentido, se debe tomar en cuenta que el teclado *"es el dispositivo más común de entrada de datos; se utiliza principalmente para introducir comandos, textos y números"*, a través de estos dispositivos *"se envían datos externos a la unidad central de procesamiento"*[328], por esa razón, cuando el sujeto activo se presenta al cajero automático e introduce el número de pin o clave secreta en el

[327] El resaltado no corresponde al original.

[328] CEDANO OLVERA, Marco Alfredo, CEDANO RODRÍGUEZ, José Antonio, RUBIO GONZÁLEZ, José Antonio, y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010, p. 55.

teclado del cajero automático, lo que técnicamente hace, es utilizar un dispositivo de entrada (teclado), mediante el cual envía datos externos a la unidad central de procesamiento.

Otra imprecisión en la que incurrió el Tribunal de Apelación en esa resolución fue la siguiente: Tal y como lo hemos visto, una modalidad de comisión de la estafa informática es el uso indebido de **datos** y no de los plásticos *("tarjetas falsas" o "clonadas")*, estos últimos sirven como dispositivos de almacenamiento de los datos, y aunque sean los instrumentos o herramientas utilizadas, simplemente son los medios o puentes mediante los cuales se consiguen usar indebidamente los datos (por ejemplo: datos financieros del ofendido que se ven disminuidos con el retiro de dinero), lo cual es al fin y al cabo, lo que exige el numeral 217 bis del CP, para su configuración en una de sus modalidades de comisión.

En el voto N° 1157-2015 de las 15:45 horas del 19 de agosto de 2015, el TASPIICJSJ, confirmó una sentencia condenatoria de dos sujetos, quienes actuaron en coautoría, si bien, en cuanto al tema de fondo el Tribunal no analizó la figura penal aplicable, lo cierto es que el caso resulta interesante, por las siguientes razones: Uno de los imputados "X" laboraba en el área del Internet Banking de un banco estatal, con vasta experiencia en sus funciones; el otro coimputado que denominaremos "Y", lo hacía para el Departamento de Contabilidad de la empresa ofendida con cuenta bancaria en el Banco en que trabajaba "X", pero no era ejecutivo de la cuenta, ni representante de la empresa en cuestión, ni tampoco estaba autorizado para manejar las cuentas bancarias de la misma. El primero de ellos, sin existir solicitud de la empresa ofendida, pero en contubernio con "Y", realizó un cambio de clave de la cuenta de la empresa ofendida para ingreso en el sistema; mientras tanto el segundo, desde una dirección IP de la empresa ofendida, hizo traslados de dinero de dicha cuenta a la suya y a la de "X". De dicha situación, se desprende que efectivamente se cometió el delito de fraude informático, ya que se manipuló el sistema informático bancario

al variar la clave de ingreso sin la autorización respectiva, y por tanto, se incidió e influyó en el mismo.

En el voto N° 480-2016 de las 14:20 horas del 30 de marzo de 2016 del TASPIICJSJ, se analizó una sentencia condenatoria en coautoría por el delito de fraude informático, las circunstancias fácticas fueron las siguientes: Un imputado se aprovechó de su labor como funcionario del INS, siendo que usó datos falsos en el sistema informático de dicha institución, manipulando de esa manera el mismo. Básicamente usó como datos falsos los siguientes: incluyó al resto de coimputados como beneficiarios de reclamos por pólizas voluntarias de automóviles sin que lo fueran; al mismo tiempo introdujo los números de cuentas bancarias personales que previamente éstos le habían facilitado; y creó la correspondiente orden de pago a favor de ellos, mediante la cual, vía SINPE les fueron girados los montos a sus cuentas bancarias personales, quienes posteriormente los retiraban. Efectivamente, nos encontramos ante un caso en el que se usaron datos falsos, los coimputados no eran beneficiarios de esas pólizas, es decir, en nuestra realidad física, esas circunstancias no eran verdaderas, independientemente que, en la realidad virtual el sistema informático las procesara. En algunos de los hechos, no se logró individualizar al funcionario del INS que influyó en el sistema informático, siendo que el Tribunal de Apelación hizo eco de la resolución del *a quo* y al mismo tiempo de la resolución N° 32-2012 de la Sala Tercera, indicó: *"…no se acredita quienes fueron las personas que materialmente manipularon el sistema informático, pero lo cierto es que los imputados con sus acciones, hicieron que llegara a buen término el plan delictivo trazado, pues una vez suministradas sus cuentas bancarias personales al funcionario del INS encargado de influir en el sistema, recibieron en éstas cuantiosas sumas de dinero, de las cuales dispusieron, siendo su actuación necesaria a los fines de consumar el tipo penal en cuestión - al ser el delito de fraude informático un tipo de estafa y por ende de resultado cortado-, y obteniendo ambos para sí un beneficio patrimonial antijurídico […] También se tiene certeza que fueron los imputados los que procedieron a hacer el retiro del dinero proveniente de esas transferencias SINPE, esto en consideración a los siguientes*

elementos: a) como regla de experiencia, las personas que van a una entidad bancaria a retirar dinero de su cuenta bancaria personal, deben presentar su cédula de identidad y estampar su firma en un documento. Los cajeros han sido preparados para detectar cualquier anomalía, no sólo con relación la cédula aportada, sino con las firmas, de manera que este resulta ser un elemento indiciario que permite derivar que en los casos que se atribuyen a […], fueron ellos quienes se presentaron a hacer los retiros de dinero que se consignan en ventanilla pues, dentro del tráfico normal de las transacciones bancarias, lo lógico es que se identifique adecuadamente a quien se presenta a realizar retiros de dinero u otras diligencias…"

Es útil también mencionar que, en el caso de uno de los coimputados, se dijo en la resolución mencionada: *"…es parte de un plan común, con funcionarios del Instituto Nacional de Seguros, para defraudar mediante su influencia en el procesamiento de datos del sistema de cómputo de la entidad afectada al introducir información falsa con el objeto de obtener un beneficio patrimonial para sí. Nótese que su función queda claramente delimitada: era dar su cuenta cliente del BAC San José, para que allí le fueran desviados fondos provenientes de distintos expedientes de siniestros cubiertos por pólizas de seguro, en las cuales precisamente mediante la* ***introducción de datos falsos en el sistema de cómputo, aparecía […] como beneficiario****, sin tener ninguna relación con la póliza respectiva ni con el siniestro ocurrido. Una vez ingresado ese dinero, el imputado lo retiraba de inmediato…"*[329]

Es claro entonces que, el sistema informático del INS fue manipulado por medio del uso de datos falsos por uno de los coautores del delito (quien era funcionario de dicha institución), y ello es lo que generó que se incluyeran falsamente como beneficiarios de reclamos por pólizas voluntarias de automóviles, al resto de coimputados, asimismo, introdujo las cuentas bancarias de imputados como beneficiarios a pesar de que no ostentaban tal condición, entonces sí nos encontramos ante la figura de la estafa informática por uso de datos falsos que

[329] Resaltado no corresponde al original.

desembocaron en la manipulación del sistema y una consecuente influencia en el mismo tanto en el procesamiento como en el resultado. Nótese que, no nos encontramos ante el supuesto de uso indebido de datos, toda vez que, el sistema informático fue alimentado con información falsa (coimputados como beneficiarios de pólizas) y no verdadera, acorde con nuestra realidad física. Después de ello, el sistema informático procesa la información, pero ya para ese momento, el imputado funcionario del INS, había incidido e influido en el mismo.

En esa misma resolución, N° 480-2016, el TASPIICJSJ al momento de analizar la figura penal de fraude informático, y como parte de sus argumentos, utilizó la resolución N° 1055-2009 de la Sala Tercera, la cual señala: *"El artículo 217 bis del Código Penal contiene la figura que en nuestro Código Penal ha sido denominada como fraude informático, nombre que no resulta ser el más acertado al ocasionar en no pocas ocasiones confusión por el término**. La palabra "fraude" hace referencia a la realización de un modus operandi que caracteriza a un determinado comportamiento, el cual se encuentra encaminado, orientado y encauzado a la obtención de un beneficio patrimonial antijurídico, propio o para un tercero, utilizando para ello el error y el ardid, acciones que resultan ser en definitiva, falsas y engañosas**. Por su parte, el fraude informático no representa cualquier tipo de acción fraudulenta que surge al utilizar un medio informático, sino únicamente cuando se refiere al perjuicio económico ocasionado a consecuencia del fraude. Entre el fraude informático y la estafa informática existe una relación de género a especie, ello presupone que toda estafa informática es un fraude informático, pero no todo fraude informático es una estafa informática. Es preferible que en lugar denominar fraude informático al ordinal 217 del Código Penal, se utilice la denominación de "estafa informática", para delimitar de mejor manera el concepto, logrando diferenciarlo del fraude informático, vocablo por demás amplio que incluye una diversidad de conductas como lo son la propia estafa, el sabotaje, los daños y el hurto informático -figura última que no se encuentra tipificada en nuestro ordenamiento- listado que no se puede considerar numerus clausus sino apertus, atendiendo a las nuevas modalidades para perpetrar delitos informáticos. El ordinal 217 bis del Código Penal, sanciona a la*

persona que influya, ya sea en el procesamiento o bien en el resultado de los datos de un sistema de cómputo, por alguno de los siguientes medios: programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema y que se realice con la intención de procurar u obtener un beneficio patrimonial para sí o bien a un tercero. Ciertamente, ninguna de las piezas acusatorias le atribuye a los encartados una conducta que haya consistido en influir en los sistemas de cómputo, sea en su procesamiento o en los resultados de los datos, o sea el cuadro fáctico no se ajusta en lo más mínimo a los elementos objetivos y subjetivos del tipo penal del numeral 217 bis del Código Penal. ***El recurrente interpreta -de modo errado- que el uso indebido de los datos constituye el delito de fraude informático, cuando más bien constituye un medio para lograr influir en el sistema de cómputo. Este último término significa una manipulación o alteración en el procesamiento o en el resultado de los datos de un sistema cómputo****, de modo que el sujeto activo logra obtener un beneficio patrimonial antijurídico para sí o un tercero. Esta manipulación se puede dar en el ingreso de los datos "insiders", en los datos de salida "outsiders" y en el procesamiento de los datos ya ingresados en una computadora o sistema informático…"*[330]

En esa resolución de Sala Tercera, nuevamente se iguala equivocadamente el verbo influir a manipular o alterar, se desconoce el motivo por el cual la Sala de lo Penal ha incurrido en esa confusión semántica. Además, el hecho de bautizar el delito como estafa, en lugar de ayudar a su comprensión, provoca tal y como lo estudiamos, todo lo contrario, ya que se desnaturaliza el significado de la palabra.

En cuanto a la distinción entre el delito de fraude informático y la actual estafa informática, en lo que respecta al agregado "influya en el ingreso", el TASPIICJSJ, en la resolución N° 587-2016 de las 09:20 horas del 22 de abril de 2016, consideró que con la redacción anterior del numeral 217 bis del CP, es

[330] El resaltado no corresponde al original.

decir, cuando era fraude informático, sí era posible encuadrar una conducta consistente en el ingreso de datos en un sistema informático, mencionó: *"Ciertamente la reforma realizada por Ley 9048 del 10 de julio de 2012 en donde se introdujeron varios delitos informáticos, y se reformó el numeral 217 bis del Código Penal, denominando la acción antes tipificada como fraude informático, como estafa informática,* ***agregó dentro de la redacción del tipo penal actual, la acción de influir en el ingreso de los datos. Esa frase, en forma específica, no estaba dentro de la redacción del fraude informático aplicable en el momento de los hechos. Sin embargo, esa mayor precisión de las conductas establecidas en el tipo penal actual, no equivale a considerar que el delito de fraude informático, dentro de las acciones que genéricamente regulaba, no contemplara la conducta realizada por los imputados consistente en que lograron imponerse por medios informáticos del usuario y contraseña de la cuenta número [Valor 002] del Banco Nacional perteneciente a la ofendida [Nombre 001] y con ello ingresaron al sistema de internet banking y trasladaron fondos de esa cuenta a sus cuentas personales. El digitar el usuario y la contraseña de esa cuenta por medio del sistema de internet banking, sin duda constituye la acción de influir en el procesamiento de datos de un sistema de cómputo, mediante el uso indebido de datos*** *que eran personalísimos y confidenciales de la ofendida para poder accesar a su cuenta bancaria vía internet..."* [331]

En ese mismo sentido se puede observar la resolución N° 1048-2018 de las 09:55 horas del 09 de agosto de 2018, el TASPIICJSJ, al realizar una comparación entre el extinto "fraude informático", y la vigente "estafa informática", tajantemente señaló: "…*Como se observa, a pesar de esta variación de ley, la conducta que se le había imputado al encartado como ilícita, según la norma vigente para el momento de los hechos (así lo dispone el principio de irretroactividad establecido en el artículo 11 del Código Penal) no varió, pues se mantuvo vigente la acción de influir en el procesamiento de datos para obtener un beneficio patrimonial para sí o para un tercero a través del uso de datos falsos…"*

[331] El resaltado no pertenece al original.

Con tales criterios, se logra determinar que, en realidad la reforma legal en cuanto a ese aspecto no era innovadora, ello en virtud de que, el delito de fraude informático sancionaba a quien influyera en el procesamiento de datos de un sistema de cómputo mediante uso indebido de datos. Entonces cabe preguntar: ¿La acción humana de usar indebidamente datos en un sistema informático estaba despenalizada para antes de la reforma del numeral 217 bis del CP? La respuesta sería negativa, ya que el elemento objetivo "procesamiento de datos", incluye evidentemente el ingreso de datos en un sistema informático, y también, el tipo penal contemplaba el *"uso indebido de datos"*, como acción humana para influir en el procesamiento de los datos, tanto es así, que inclusive en la resolución analizada, de manera correcta se aplicó la figura penal del fraude informático. No creemos que haber introducido el verbo manipular, permitiera precisión al tipo penal, ni tampoco que se agregara la frase *"en el ingreso"*, más bien, esa reforma legislativa, crea confusión, siendo que partió de una premisa falsa, al considerar que el ingreso de datos estaba despenalizado, cuando ello no era así. Inclusive, el tipo penal hace referencia al procesamiento, el cual se presenta desde la misma fase de ingreso de datos, cuando se hace la validación de ellos, por lo tanto, el artículo de antaño no excluía esa fase de ingreso.

En cuanto a la participación del sujeto que presta la cuenta bancaria y posteriormente, hace los retiros de dinero desde cajeros automáticos, se hace necesario analizar cada caso según sus características propias, para poder concluir si se está ante un coautor o un partícipe (cómplice o instigador). En la resolución N° 2016-690 de las 15:30 horas del 10 de mayo de 2016, el TASPIICJSJ, ordenó el reenvío bajo el siguiente análisis: *"…Desde un inicio de la investigación, la Fiscalía estableció de manera muy clara que el encartado […] no influyó en el manejo o procesamiento de datos, para efectos de ser el autor directo de la sustracción electrónica del dinero de la cuenta perteneciente a la ofendida [Nombre 004], sino que su participación consistió en facilitar su cuenta bancaria y presentarse a retirar los fondos de la misma, para disponer libremente de ellos.* ***En este plano de la participación, el Tribunal es omiso en desarrollar si el encartado logra alguna condición, sea de coautor o cómplice, según el caso,***

con el solo hecho de prestar su cuenta para recibir el dinero sustraído[332]*, siendo lógico que no necesariamente por una participación de ese tipo tendría equipo de cómputo en su poder capaz de realizar las transacciones investigadas..."*[333] Nos encontramos eminentemente ante un tema probatorio, en cuanto al nivel de participación del imputado, ya que *per se*, el hecho de recibir el dinero en la cuenta y posteriormente hacer los retiros, no implica necesariamente que se está ante un coautor, ello en razón de que, el plan previo y la distribución de funciones debe ser probada en juicio. Lo que sí resulta importante del voto, es que no necesariamente se es coautor, ya que cabe la posibilidad de ser tomado como partícipe, pero ese análisis debe ser casuístico y plasmarse en las sentencias.

En el voto N° 617-2017 de las 14:20 horas del 26 de mayo de 2017, el TASPIICJSJ, anuló una sentencia condenatoria por los delitos de estafa informática y robos agravados, caso en el que actuaron varios coautores, quienes en tesis de principio rompieron las ventanas de unos vehículos y sustrajeron tarjetas de crédito de las víctimas, las cuales posteriormente fueron utilizadas en locales comerciales, por medio de un datáfono; se acusó además que, uno de los sujetos activos fungía como administrador del local comercial, recinto al cual acudieron los otros coimputados a comprar mercadería con las tarjetas de crédito sustraídas, las cuales no les pertenecían. Consideró dicho Tribunal que esas acciones podrían configurar el delito de estafa general, y no de fraude informático, argumentó el *ad quem*: *"…la resolución impugnada, está cargada de una serie de falencias en torno a los casos de los imputados […] en lo referente a los hechos que se calificaron por el a quo como fraude informático, ya que la ausencia de fundamentación en tal sentido es también evidente […] la base fáctica y jurídica*

[332] El resaltado no corresponde al original.

[333] En ese mismo sentido: El TASPIICJSJ, en la resolución N° 1818-2019 de las 10:05 h del 11 de octubre de 2019, apoyándose en la resolución N° 587-2016 de las 09:20 h del 22 de abril de 2016, emitida por el mismo Tribunal, anuló la sentencia absolutoria dictada por el *a quo*, argumentando que el delito de estafa informática atendiendo el caso en concreto admite la coautoría para aquel imputado que: en primer lugar, presta la cuenta bancaria, como cuenta destino del dinero que es sustraído de la cuenta bancaria de la parte ofendida, mediante la influencia o manipulación del sistema informático; y que, en segundo lugar, hace los retiros de dinero del cajero automático.

con base en la que se condenó a tales justiciables por los delitos de robo agravado, está íntimamente relacionada en tales vertientes con la condenatoria que se les impuso por los eventos que el Tribunal calificó como estafa informática, calificación que desde ya debe indicarse que no se sustentó debidamente en el fallo, y que jurídicamente no corresponde al marco fáctico acreditado, ya que es evidente que no hubo alteración o manipulación de un sistema informático, sino que en palabras sencillas, según dicha relación de hechos probados, ***lo que se hizo fue utilizar fraudulentamente un instrumento de pago, sea una tarjeta de crédito al hacerse pasar quien la utilizó como su titular, lo cual no es un falseamiento de la realidad en aras de obtener un beneficio patrimonial antijurídico, lo cual se engloba en la norma del artículo 216 del Código Penal, es decir, en el delito de estafa*** *[…] Además, tal y como se señala por las recurrentes, el delito de estafa informática regulado en el numeral 217 bis del Código Penal, lo que tipifica es la manipulación y alteración de un sistema informático con el objetivo de obtener un beneficio patrimonial antijurídico por el agente activo. En la especie, conforme a la relación de hechos probados de la resolución de marras, lo que se colige es que se utilizó una tarjeta de crédito verdadera previamente sustraída a su legítimo poseedor, la que se "pasó" por el datáfono correspondiente como un medio de pago de una mercadería que, supuestamente, se adquiría legítimamente en la tienda […] Tal conducta no implica en modo alguno la manipulación o alteración del sistema financiero de los entes bancarios relacionados con la tarjeta de crédito, sino, únicamente, significó la utilización indebida de una tarjeta de crédito por parte de una persona que no era su titular, es decir, lo que se dio fue un engaño o ardid que produjo un beneficio patrimonial antijurídico para el agente activo de la conducta […] Lo anterior, como bien lo señalan las recurrentes, constituiría un delito de estafa conforme a lo establecido en el artículo 216 del Código Penal, siendo que por el monto de lo que se estableció como defraudado, sería una estafa menor."*[334]

Del razonamiento utilizado por el Tribunal, se desprenden varias circunstancias insoslayables:

[334] Resaltado y subrayado no corresponde al original.

1. A pesar que, a los coimputados se les condenó por “estafa informática” (tipo vigente al momento de comisión de los hechos), quienes resolvieron, utilizaron indiscriminadamente los conceptos “fraude informático” y “estafa informática”, sin lugar a dudas, es importante utilizar un lenguaje preciso en las resoluciones judiciales, más sabiéndose que se está produciendo jurisprudencia nacional, por ende utilizar los dos conceptos de manera indistinta, genera confusión, ya que no son exactamente lo mismo, tal y como se ha expuesto en el presente trabajo.

2. El Tribunal realizó un análisis confuso al afirmar que, usar una tarjeta bancaria haciéndose pasar como verdadero titular *“no es un falseamiento de la realidad”*, pero de seguido, señala que esa conducta constituye una estafa general de las previstas en el numeral 216 del CP, dicho razonamiento es contradictorio.

3. Pareciera que el Tribunal consideró que se incurre en una estafa convencional cuando se usa indebidamente la tarjeta de crédito en una máquina.

4. El Tribunal evidenció una confusión importante en el tratamiento del delito de estafa informática, ya que lo entiende únicamente en su dimensión de manipulación o alteración del sistema informático, invisibilizando la influencia en el procesamiento mediante el uso indebido de datos.

En realidad el 217 bis del CP, lo que tipifica como verbos son: *“uso de datos falsos o incompletos, **el uso indebido de datos**, programación, valiéndose de alguna operación informática o artificio tecnológico”*, de manera que se incida, influya en un “sistema automatizado de información”, entonces no es cierto lo afirmado por el Tribunal de Apelación, en cuanto a limitar el tipo penal, diciendo que únicamente “***tipifica la manipulación y alteración de un sistema informático”***, esa premisa incompleta de la que se parte, provocó que se dejara

de lado el elemento objetivo del tipo penal “uso indebido de datos”, como mecanismo que influye en un sistema informático, y es que en el caso de estudio, eso fue lo que en apariencia sucedió, ya que, el sujeto activo “*utilizó una tarjeta de crédito verdadera previamente sustraída a su legítimo poseedor, la que se “pasó” por el datáfono correspondiente como un medio de pago de una mercadería que, supuestamente, se adquiría legítimamente en la tienda”*.

Además, el Tribunal incurre en otro error en el razonamiento, mencionó que esa acción humana provoca un engaño o ardid, sin embargo, no precisó según su perspectiva, quién o qué es objeto de la acción engañosa, no indicó si se refiere a la máquina (sistema informático), al titular verdadero de la tarjeta bancaria, o inclusive al cajero humano que atiende al sujeto activo; en los primeros dos supuestos, la afirmación sería equivocada, ya que a una máquina no se le puede engañar, y el titular de la tarjeta atendiendo la mecánica de los hechos no ha sido objeto de engaño (la sustracción de tarjetas fue mediante la tacha de un automotor); en cuanto al último supuesto, no es aplicable al caso en concreto, toda vez que según la Fiscalía y la sentencia del *a quo*, el administrador de la tienda que pidió la identificación, y que usó la tarjeta en el datáfono, era un coautor, es decir, sería ilógico que fuese engañado por su compañero de actuación, entonces su condición de coimputado en tesis de principio, elimina la posibilidad de que hubiese sido engañado en daño de un tercero (titular de la tarjeta o entidad bancaria). Esa confusión en la resolución analizada, se acentúa más cuando la cámara de apelación mencionó con respecto a las acciones del coautor (administrador del local comercial): *“…no pueden englobarse o tipificarse en el artículo 217 bis del Código Penal, es decir, el delito de fraude informático* (sic)*. Esto, por cuanto como ya se ha señalado previamente en el presente pronunciamiento […] no manipuló o alteró sistema informático alguno, ya que su conducta se limitó a utilizar dos tarjetas de crédito verdaderas y con datos originales (en dos ocasiones distintas), según la pieza acusatoria,* ***a sabiendas de que quien las utilizaba no era su verdadero titular****. Así las cosas, lo que se daría en caso de confirmarse la hipótesis fiscal sería una estafa menor, ya que lo*

que lo que está de por medio es la deformación de la verdad mediante un engaño con el fin de obtener un beneficio patrimonial antijurídico".

Se evidencia nuevamente lo que se ha venido sosteniendo, si el administrador de la tienda sabía que quien utilizó la tarjeta no era el verdadero titular (se confirma tesis fiscal), *ergo* no pudo ser engañado y en consecuencia, se excluiría el delito de estafa general, sin embargo, esa situación no excluye la posibilidad de subsumir la conducta en el delito de estafa informática, por la influencia en el sistema informático mediante el uso indebido de datos almacenados en la banda magnética de la tarjeta utilizada, punto que fue inobservado por el Tribunal de Apelación en el análisis intelectivo de su resolución. Ahora bien, en el supuesto que, el dependiente no estuviera actuando en contubernio con quienes llegaron a usar las tarjetas de crédito, podría subsistir una estafa triangular, siempre y cuando hubiera sido inducido a error mediante un engaño relacionado con la identidad del verdadero titular de la tarjeta de crédito.

Por otro lado, en la resolución N° 851-2017 de las 08:52 h del 12 de julio de 2017 del TASPIICJSJ (mencionada párrafos atrás), se sigue la misma tónica que hemos expuesto, el *ad quem*, a pesar que, para la fecha de comisión de los hechos, el delito juzgado fue "estafa informática" (así lo indicó expresamente el Tribunal *a quo*), en algunas ocasiones se decantó por denominarlo "fraude informático", aspecto del todo incorrecto si atendemos a un correcto uso de los conceptos jurídico penales, indicó: *"…El tribunal expresó claramente sus argumentos de por qué consideró que los hechos probados debían ser calificados como un Fraude informático, (artículo 217 bis del Código Penal) y así lo explicó en su sentencia, fundamentación que ésta Cámara avala.* ***Se determinó que el imputado insertó información electrónica falsificada en sus bandas magnéticas, con lo que logró vulnerar los sistemas de seguridad de los datafonos*** (sic)***, logrando así, la aprobación de las transacciones con plásticos clonados. Ya que, producto de dicha acción, logró manipular en forma indebida el sistema informático en las entidades bancarias, lo que se adecua a la conducta tipo que establece la norma*** *[…] Siendo que en el*

presente caso, existió una clonación de datos hacia un plástico, ***el cual fue utilizado como instrumento para manipular el sistema de acreditación de tarjetas de crédito****, información que fue clonada por medio de un "skimer"* (sic)*…"* De dicho análisis se evidencia un error conceptual, ya que en realidad no nos encontramos ante una manipulación del sistema informático, lo que existió fue una influencia en el sistema informático, y aunque pueda parecer un tema meramente baladí, en realidad no lo es, deviene en fundamental visibilizarlo, puesto que conforme al principio de legalidad, tal y como se ha expuesto en el presente trabajo, tanto "manipular" como "influir", son verbos diferentes, que regulan distintas situaciones fácticas.

En esa resolución, también se realiza un análisis interesante, el cual comparto, relacionado con el concurso aparente de delitos entre la estafa informática y otras figuras, señaló el TASPIICJSJ: *"…resulta evidente que, la norma tipo aplicable resulta ser la aquí citada, y no, la establecida en el numeral 373 definida como falsificación de moneda, o valores equiparados, conforme a lo establecido en el artículo 375 que indican "Para los efectos de la aplicación de la ley penal quedan equiparados a la moneda: 1) El papel moneda y de curso legal nacional o extranjero; 2) Las tarjetas de crédito o de débito; 3) Los títulos de la deuda nacional o municipal y sus cupones; 4) Los bonos o letras de los tesoros nacional o municipal; 5) Los títulos, cédulas y acciones al portador, sus cupones y los bonos y letras emitidas por un gobierno extranjero; 6) La moneda cercenada o alterada; y 7) Las anotaciones electrónicas en cuenta, ello relacionado con el numeral 372, todos del Código Penal.* ***Como se observa, la conducta a grandes rasgos se adecua a lo establecido en el numeral 373, relacionado con el 375 y 372, todos del Código Penal, empero la prioridad de aplicación de éstas normas, decae, cuando el ordenamiento jurídico cuenta con un tipo penal mas*** (sic) ***específico o especial, y es lo que en éste caso sucede, con relación al delito del numeral 217 bis, titulado como fraude informático*** (sic) *[…] De allí que el Tribunal tenía por imperativo de ley, el tipo especial, "fraude informático" y no "valor falso equiparado"…"* Si bien los artículos 372, 373 y 375 del CP, se encuentran en el Título XVI denominado *"Delitos contra la fe pública"*, mientras

tanto la estafa informática del numeral 217 bis se ubica en el Título VII de *"Delitos contra la propiedad"*, ésta última en su redacción, como factor normativo, no sólo es más especial, también integra a los primeros tres, por lo tanto, nos encontramos ante un concurso aparente de normas por criterio de especialidad y de consunción según el artículo 23 del CP, que es lo que al fin y al cabo aplicó, sin decirlo el TASPIICJSJ.

En ese mismo sentido, el TASPIICJS en la resolución N° 2030-2014 de las 10:00 horas del 15 de octubre de 2014, confirmó la sentencia del *ad quo*, en el tanto condenó al agente por el delito de fraude informático y absolvió a otros imputados. A pesar de ello, la jueza Rosaura Chinchilla Calderón, emitió voto de minoría con el cual estoy de acuerdo, que ordenaba el juicio de reenvío, en lo que interesa ella mencionó: *"No obstante, sí concuerdo con el recurrente, en que la sentencia no analizó otras posibilidades de adecuación típica de los hechos acusados. Específicamente, no se fundamentó adecuadamente sobre el uso de documento falso que cada uno de estos encartados habría hecho, al utilizar una tarjeta con sus nombres pero cuya información, contenida en la banda magnética, era de otra persona, lo que a ellos les constaba, según la pieza fiscal. Esa conducta está prevista en el numeral 372 del Código Penal y,* ***aunque inicialmente se calificara la conducta de un fraude informático, tal figura recoge, por concurso aparente, otros delitos que, en caso de desaparecer la primera, hace que resurjan los tipos subsumidos (artículo 23 del Código Penal), nada de lo cual fue objeto de análisis****. Por ello, en mi criterio, procede acoger el recurso y anular la absolutoria de ambos encartados…"* Es atinado dicho comentario en razón de que, el fraude informático en muchas ocasiones concurre aparentemente con otros delitos, siendo precisamente la labor del juez o la jueza, delimitar dichas situaciones, para realizar una aplicación adecuada de la ley. Inclusive, ese mismo razonamiento termina siendo aplicado cuando la estafa informática retrocede por concurrir aparentemente con la estafa general.

Por otro lado, en la resolución N° 197-2018 de las 09:30 horas del 16 de febrero de 2018, el TASPIICJSJ, remitiéndose al sitio web *https://www.segu-*

info.com.ar/malware/phishing.htm, consideró como un fraude informático el *"phishing"*, indicó: "…*es definido como una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombre de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima…"*

Mediante la resolución N° 1899-2018 de las 08:20 horas del 21 de diciembre de 2018, el TASPIICJSJ, al resolver un recurso de apelación interpuesto por el Ministerio Público, remitiéndose a las resoluciones números: 208-2009 de las 10:55 horas del 06 de marzo de 2009; 148-2006 de las 09:00 horas del 24 de febrero de 2006; y 763-2006 de las 09:20 horas del 18 de agosto de 2006, todas de la STCSJ, indicó con respecto a los verbos "manipular" e "influir" del numeral 217 bis del CP: *"…la Sala Tercera […] interpretó que, en este tipo penal, el verbo "influir" se debe entender como sinónimo de "manipular" y que, básicamente, el delito de estafa informática requiere de algún manejo de programas que afecte el proceso de datos del sistema. Así, en la primera de las resoluciones antes indicadas, se dijo lo siguiente: "Por su parte, la conducta tenida por acreditada, en el caso en estudio, es el apoderamiento ilegítimo de dinero ajeno, utilizando la tarjeta original, por medio de un ordenador, pero sin modificación, ni alteración de la información que éste contenía, de modo que indujera a error en el procesamiento o el resultado de los datos del sistema. La acción realizada es la misma que hubiera hecho la titular de la tarjeta de débito, para obtener el dinero, por lo cual la conducta tenida por cierta no se adecua al tipo penal considerado por el Tribunal". Si bien el delito en comentario fue modificado en el año 2012, las conductas añadidas en dicho cambio no fueron imputadas por el Ministerio Público para el caso concreto y, en lo que respecta a este, la redacción del tipo penal para el momento en que se hizo dicho análisis ("Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema") no incluyó ninguna alteración, por lo que se*

*mantiene vigente la sinonimia de "influir" como "manipular". **De toda suerte, aunque no se comparta la tesis de equivalencia entre ambos verbos y que se estime que constituyen acciones independientes, en este caso, es intrascendente si el encartado manipuló el procesamiento de los datos en los sistemas informáticos de las emisoras de las tarjetas, en virtud de que las tarjetas de crédito y débito eran originales y no estaban adulteradas**. De modo que, lo esencial, es determinar la influencia que ejerció el justiciable en el resultado de los datos del sistema bancario de las distintas entidades que emitieron la tarjeta mediante la utilización fraudulenta que hizo de ella, con el propósito de adquirir ilegítimamente bienes a través de una transacción no autorizada por el tarjetahabiente. Aquí es donde radica el tema central de la discusión que plantea la apelante, en razón que esa **influencia** se pretende sustentar en el empleo que efectuó el dependiente del comercio, como un instrumento no doloso, al engañarlo de que era el verdadero titular de la tarjeta de crédito. De manera que fue un tercero, influido por el inculpado de que su identidad correspondía al tarjetahabiente, la persona que manipuló el datáfono para transmitir, al banco emisor de la tarjeta de crédito, la información de que su titular solicitaba la transacción correspondiente para el pago de un bien, cuando ello no era así…"* [335]

Nótese como en dicha resolución, por la mecánica de los hechos, al haberse utilizado plásticos originales, se descartó que el imputado manipulara el sistema informático, de manera correcta se indica que lo que pudo existir fue una influencia en el sistema, en razón de que se indujo a error al dependiente del comercio, quien es el que en definitiva se vio engañado por el imputado al creer que era el verdadero titular de la cuenta, y usó la tarjeta como medio de pago, para realizar la operación bancaria mediante un datáfono.

De manera acertada, el *ad quem* señala que lo que existe en el caso en concreto es una estafa general, en razón de que, se indujo a error al dependiente, simulando el sujeto activo ser el legítimo propietario de la tarjeta bancaria cuando

[335] Subrayado y resaltado no corresponden al original.

en realidad no lo era, en ese sentido, mencionó: *"Ese engaño que sufrió el dependiente del comercio es el propio de la estafa pura y simple, no de la informática, en virtud de que la manipulación del sistema informático lo efectuó una tercera persona quien actuó sin dolo defraudatorio. En este asunto,* ***la conducta acreditada es el engaño que realizó el justiciable hacia el dependiente del establecimiento comercial, al hacerle creer falsamente que era el titular de la tarjeta de crédito, cuando no lo era, para así poder utilizar dicho instrumento como forma de pago de distintos bienes, pero sin modificar ni alterar la información que contenía dicha tarjeta, pues ella era original, por lo cual la conducta tenida por cierta no se adecua al tipo penal de la estafa informática****…"* [336]

Pareciera ser que el reclamo planteado en el recurso, pretendía que se considerara una especie de autoría mediata en el caso en concreto, es decir, que el dependiente actuó como un instrumento con un déficit de imputación en cuanto al dolo, por lo tanto, el sujeto activo sí influyó en el sistema informático, pero como "el hombre o la mujer de atrás". Si bien y de forma general, se puede afirmar que nada impide que pueda cometerse una estafa informática mediante autoría mediata, lo cierto es que, en el caso concreto se configuraron tanto los elementos objetivos como subjetivos del tipo penal 216 del CP, artículo que resulta más específico para la situación fáctica juzgada.

En la resolución N° 1431-2019 de las 16:10 horas del 19 de agosto de 2019, el TASPIICJSJ, ante un recurso de apelación de sentencia interpuesto por el Ministerio Público, anuló parcialmente una sentencia absolutoria del Tribunal Penal del Primer Circuito Judicial, aduciendo que existió falta de fundamentación, el caso consistió en que el sujeto activo de la conducta falsificó tarjetas de crédito, consignando sus datos personales en dichos soportes plásticos, además las usó haciéndose pasar como el verdadero titular de la información contenida en las bandas magnéticas, con la finalidad de obtener un beneficio patrimonial antijurídico, en ese sentido mencionó la cámara en alzada: *"tampoco se explica en*

[336] Resaltado no corresponde al original.

la resolución examinada el motivo por el cual la "finalidad" del autor excluye la aplicación de los artículos 373 (Falsificación de moneda) y 375.2 (Valores equiparados a moneda) del Código Penal. En la solución propuesta por el tribunal de juicio pareciera haber implícita una aplicación de las reglas del concurso aparente de normas (artículo 23 del Código Penal), pero no se da una razón por la cual solo debe aplicarse el artículo 217 bis del Código Penal, téngase presente que el bien jurídico tutelado por el artículo 217 bis es el patrimonio, mientras que las figuras previstas en los artículos 373 y 375 son delitos contra la fe pública, ***por lo que el tribunal debió explicar por qué el delito de estafa informática comprende en sí todo el disvalor de la conducta realizada por el encartado, pues era su deber hacer pronunciamiento fundado sobre todas las cuestiones planteadas en el debate, como lo es lo concerniente a la calificación jurídica (artículos 142 y 361 del Código Procesal Penal)****, sobre lo cual el representante del Ministerio Público sostuvo la tesis de que se estaba en presencia de dos delitos de falsificación de valores equiparados a moneda, conforme a la relación de los artículos 373 y 375 inciso 2° del Código Penal…"*[337]

En los supuestos fácticos, en los cuales el imputado se presenta a un local comercial y sin identificarse ante el dependiente, paga con una tarjeta bancaria, cuyo titular es otra persona, resulta de utilidad plantear la siguiente interrogante: ¿Es posible que el sujeto activo a través de un acto concluyente pueda engañar al dependiente del establecimiento? La respuesta es afirmativa, en ese sentido, el profesor Francisco Castillo considera: *"Nosotros pensamos que la estafa no es un delito de expresión y que puede cometerse por manipulación de instrumentos o de objetos, si tal manipulación tiene influencia sobre el cuadro de representación de quien se equivoca, es decir, del sujeto pasivo de la estafa […] Un engaño mediante comportamiento concluyente existe cuando el autor no manifiesta un hecho contrario a la verdad espressis verbis, sino que ello resulta de las circunstancias en que se desenvuelve su comportamiento. Para que exista un engaño mediante un comportamiento concluyente el comportamiento total del*

[337] Resaltado no corresponde al original.

autor, de acuerdo al tráfico común, debe tener un valor expresivo de la afirmación de un hecho. Este comportamiento se transmite al receptor, que lo interpreta según las reglas del tráfico común, como un hecho."[338]

Según las reglas comerciales y de seguridad, la única persona autorizada a utilizar la tarjeta bancaria es su verdadera titular, y es desde esa realidad que se debe partir, precisamente por esa razón, el dependiente del local, al ver que la persona va a pagar con el plástico, debería en tesis de principio suponer, que se trata del verdadero dueño del instrumento de pago. El sujeto activo en su psiquis conoce que ello no es así, siendo su finalidad inducir en error al dependiente para que le permita usar el plástico y así causarle un perjuicio patrimonial a un tercero. El imputado simula ante el dependiente estar utilizando una tarjeta que le pertenece, él muestra y utiliza una tarjeta que no integra su patrimonio, por eso podría existir un engaño, que hace incurrir en error al dependiente. Ya que, si no simulara dicha situación, el dependiente teóricamente debería impedir que se materializara la compra. Por lo tanto, podría considerarse que el sujeto activo hace nacer en el dependiente la errónea creencia de ser el titular del plástico y consecuentemente tener capacidad para pagar. En principio, los hechos suceden en un establecimiento comercial, en donde el dependiente sabe que puede vender únicamente a quien sea el titular de la tarjeta.

Lo anterior es una situación que debe ser valorada, para poder deslindar de manera precisa, si nos encontramos ante una estafa informática o una estafa convencional. Es necesario, sin embargo, hacer un análisis caso por caso, para poder determinar si existió o no un engaño hacia el dependiente del establecimiento comercial.

Señala el autor Javato Martín desde el derecho penal español lo siguiente: *"…Mucha más incidencia práctica que los anteriores presentan los supuestos llevados a cabo por terceros no titulares de tarjetas. Entre ellos se suelen incluir la utilización no consentida de la tarjeta por el tercero para obtener alguna cantidad*

[338] CASTILLO GONZÁLEZ, Francisco. *El delito de estafa*. Editorial Jurídica Continental, San José, 2ª ed. 2013, pp. 153 y 155.

de dinero en una entidad financiera o para realizar el pago de productos o servicios adquiridos directamente en un establecimiento comercial. A juicio del autor, ninguna dificultad existe para incardinar semejantes hechos en el art. 248.1 del Código Penal, pues quien finge ser titular de una tarjeta de debido o crédito en una operación presencial para lograr la entrega de ciertos bienes o la prestación de algún servicio estaría creando una falsa apariencia de crédito con la presentación de la misma frente al comerciante o empleado. Lo mismo cabría predicar respecto a la utilización de otros medios de pago, de menor aceptación, como la tarjeta monedero, el pago mediante el teléfono móvil, los cheques electrónicos o el dinero electrónico en sentido estricto, siempre claro está que se empleen en una relación comercial directa y personal. Estima el autor, sin embargo, que la admisión del delito de estafa aparece condicionada a la observancia por parte del comerciante de la diligencia exigible por los usos mercantiles, que debe ponderarse de acuerdo a una valoración de lo que constituye la práctica habitual en el sector profesional de que se trate…"[339] El profesor Castillo González refiere que *"Cuando el que maneja el sistema hace un acto dispositivo a raíz de un engaño, utilizando los medios del procesamiento de datos sobre el patrimonio ajeno, entonces nos encontramos ante una estafa general, realizada de manera triangular."*[340]

Sin lugar a dudas, son múltiples las formas en que se puede hacer uso indebido de datos, casi imposibles de enumerar, situación que se complica aún más con los avances de la tecnología. En la actualidad, por ejemplo, las dinámicas de pago con tarjetas en establecimientos comerciales son muy variadas, ya ni siquiera se requiere introducir o deslizar la tarjeta de crédito en el datáfono, ahora basta simplemente acercar el plástico a dicho dispositivo, para poder concretar la transacción. Inclusive, ni siquiera es necesario entregar la tarjeta al cajero, puesto

---

[339] JAVATO MARTÍN, Antonio Mª. *Sobre: "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"*. En: Revista Electrónica de Ciencia Penal y Criminología. N° 10-r5, ISSN 1695-0194, Valladolid, 2008, p. 4. Versión electrónica en: http://criminet.ugr.es/recpc/10/recpc10-r5.pdf.

[340] CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016, p. 122.

que el cliente termina siendo quien aproxima la tarjeta al citado aparato. Este amplio abanico de conductas representa retos intelectivos para los operadores del derecho, quienes necesariamente deben estar informados sobre los avances tecnológicos, para comprender de mejor manera los sucesos.

Tal y como se pudo observar en la jurisprudencia, han existido errores conceptuales relevantes que inciden notablemente en la calidad de las resoluciones. De esa manera se desprende que, introducir la informática en el derecho no ha sido tarea fácil, y para brindar una justicia cumplida, es esencial, permanecer en constante aprendizaje.

Conclusiones

Mientras redactaba la presente investigación, a nivel mundial en pleno apogeo se desarrollaba la pandemia por Coronavirus SARS-CoV-2, emergencia sanitaria que impactó y varió de forma notoria y drástica la rutina diaria de las personas, aumentando el uso y la dependencia del ser humano hacia la tecnología, ello en diferentes campos, como lo son: el comercio, recreación, educación, salud, ámbito laboral, y otros; precisamente ese incremento desmedido en el uso de aparatos y medios electrónicos, se convierte, tal y como se determinó en la investigación, en caldo de cultivo que aumenta la esfera de riesgo en que se desenvuelve el ser humano en la web, exponiéndolo a ser víctima de múltiples delitos, entre ellos los de índole patrimonial o que vulneran su privacidad, intimidad e incluso su autodeterminación informativa.[341]

Ahora bien, como principales conclusiones del presente trabajo de investigación se obtuvieron las siguientes:

1. La estafa informática tipificada en el artículo 217 bis del CP, introducida mediante la ley N.º 9048 del 10 de julio de 2012, titulada: *"Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal"*, publicada en el Alcance N.º 172 de La Gaceta N.º 214 del 06 de noviembre de 2012, no es una verdadera estafa puesto que carece de los elementos para ello, lo que sí es que, resulta una construcción legislativa, cuya intención es sancionar conductas humanas relacionadas con el uso de datos en sistemas informáticos, tutelando principalmente el bien jurídico patrimonio, sin embargo, se trata de un delito pluriofensivo, en el cual podrían englobarse otros bienes jurídicos como la autodeterminación informativa y la misma integridad del sistema automatizado de datos.

---

[341] Ver La Nación. *"Denuncias por fraudes electrónicos en la banca crecieron 36% hasta octubre de 2020"*. Consulta realizada el 23 de noviembre de 2020, en sitio web: https://www.nacion.com/economia/banca/denuncias-por-fraudes-electronicos-en-la-banca/IOXOM53RM5E35DK5LQ5NIM34XI/story/ .

2. La estafa informática dista de la estafa general prevista en el numeral 216 del CP, ya que prevé situaciones fácticas completamente distintas, es claro que la primera no contempla dentro de sus elementos objetivos del tipo, un engaño ni un hacer inducir a error, ni una persona engañada que se autolesiona en su patrimonio; lo que sí describe, es una especie de apoderamiento del patrimonio de la víctima o la obtención de un beneficio ilícito por parte del sujeto activo; básicamente, esa característica que se encuentra íntimamente relacionada con el bien jurídico tutelado y el título de "estafa", son las únicas similitudes con la estafa convencional. La estafa informática al no contener dentro de sus elementos objetivos el engaño, el *nomen iuris* de dicho numeral deviene en erróneo y tiende a la confusión, siendo recomendable como una proposición de *lege ferenda*, una variación en su nomenclatura, para facilitar la comprensión a las personas usuarias del sistema judicial e incluso a quienes operamos el derecho.

3. Del estudio realizado, se desprende que la redacción y los elementos objetivos tanto descriptivos como normativos, integrados en el tipo penal 217 bis del CP, denotan ser confusos, lo cual repercute negativamente, puesto que no facilita la comprensión del mismo; ello sumado al hecho que lo descrito se relaciona directamente con los campos de la informática y las nuevas tecnologías, nos permite concluir que nos encontramos ante una delincuencia no convencional, vale aclarar que, esa no convencionalidad es parcial, puesto que se vincula con formas específicas de comisión. Ciertamente, el delito de interés prevé diversas formas de incurrir en él, siendo que, en la praxis judicial, a quienes más se les vincula con el ilícito, son aquellas personas que prestan o facilitan sus cuentas bancarias para recibir los fondos de las víctimas (cuentas destino); o aquella persona que usa de forma indebida una tarjeta bancaria y la clave de acceso en un cajero automático; o la utiliza para una compra sin inducir a error al dependiente. Esos comportamientos humanos no se encuentran teñidos por una mayor complejidad en su ejecución ni tampoco para investigarlos, tal vez, décadas atrás pudieron ser considerados poco ortodoxos, sin

embargo, en la actualidad se recurre a ellos con suma frecuencia. No obstante lo anterior, la no convencionalidad de la estafa informática, sí se logra desprender de la forma de comisión del delito, relacionada con la programación o valerse de una operación informática o artificio tecnológico que incida en el procesamiento de datos, en dichos supuestos se dificulta demostrar la identidad del autor, quien realiza la acción de forma anónima dentro del ciberespacio, si bien podría ubicarse el dispositivo desde el cual se realizó el comportamiento, lo cierto es que, representa nuevos retos tanto para quienes operan el derecho como para quienes investigan. Esas dificultades, son las que permiten considerar a la estafa informática como no convencional en ciertas formas de comisión.

4. La estafa informática en su forma de comisión simple, prevé como pena mínima 3 años de prisión, extremo inferior que está muy por encima de los mínimos de prisión previstos en abstracto en la estafa general del artículo 216 del CP, en cualquiera de sus modalidades: 2 meses (pena base), 2 meses y 20 días (pena base aumentada en un tercio), 6 meses (pena agravada) y 8 meses (pena agravada aumentada en un tercio). Se evidencia entonces, una desproporción importante, ya que a pesar de que ambos tipos penales, teóricamente tutelan el mismo bien jurídico, las consecuencias procesales para quien deba descontar esas penas serán muy distintas, aun y cuando sean impuestos extremos mínimos, por ejemplo, con relación a beneficios en la etapa intermedia, fase de juicio o en etapa de ejecución de la pena, así como con respecto al plazo que durará inscrita la sentencia en el Registro Judicial. En su forma de comisión agravada, el extremo mínimo a imponer previsto en abstracto es de cinco años de prisión, superando en demasía cualquiera de los extremos menores previstos para la estafa general, ya sea de menor o de mayor cuantía.

5. La estafa informática a diferencia de la estafa general, no establece dentro de sus elementos objetivos del tipo, una distinción en la pena a imponer

según el monto defraudado, es decir, no atiende el principio de lesividad. Además, el 217 bis del CP, contraria el principio de proporcionalidad, por cuanto a pesar de encontrarnos ante un delito que permite cuantificar el daño (en tanto protege primordialmente el bien jurídico patrimonio) no diferenció las penas según las cuantías defraudadas, lo que obliga la imposición de una pena elevada, aun y cuando el eventual daño patrimonial ocasionado sea nimio. Es por ello que, de *lege ferenda*, se propone que con la finalidad de encontrar coherencia en el ordenamiento jurídico y evitar penas desproporcionadas para lesiones ínfimas al patrimonio, se dispongan penas diferenciadas según la cuantía defraudada, siguiendo los parámetros del artículo 216 del CP.

6. Según el análisis jurisprudencial realizado, se desprende que el agravante previsto en el artículo 217 bis del CP, desde un punto de aplicación del derecho, se convierte en la regla y no la excepción, ello ya que sanciona con mayor pena cuando las acciones son cometidas en contra de sistemas de información públicos, sistemas de información bancarios y de entidades financieras, siendo esas, sin lugar a dudas, las modalidades de comisión más frecuentes en la sociedad actual, lo que incide directamente en las salidas alternas al proceso y por lo tanto en los mismos intereses de las víctimas, por ejemplo: El agravante de la estafa informática al prever una pena mínima de 5 años de prisión, *prima facie*, impide conceder el beneficio de ejecución condicional de la pena, por lo tanto, es un obstáculo para la aplicación de la conciliación, negándoles a las partes intervinientes poder solucionar el conflicto de manera pacífica. En virtud de lo anterior, de *lege ferenda*, se propone que los extremos mínimos de la pena en abstracto de la estafa informática sean reducidos, para de esa manera aplicar salidas alternas al proceso y satisfacer los intereses de las víctimas, así como que se elimine la agravante en función del sistema informático atacado.

7. El verbo típico del artículo 217 bis del CP, es el uso de datos, mediante el cual se influye en el sistema informático; el hecho de insertar en el tipo

penal el verbo “manipular”, fue innecesario, puesto que, el extinto delito de fraude informático (antiguo numeral 217 bis del CP, vigente hasta antes del delito de estafa informática) sí preveía el verbo influir, modo infinitivo amplio, el cual permitía y permite en la actualidad contemplar incluso la fase de ingreso de datos en el sistema informático, y es que, es evidente que no se puede influir en un sistema automatizado de datos si no es introduciendo datos en él. El verbo influir, contiene ya de por sí el verbo manipular, ello sin importar si nos encontramos ante datos falsos o incompletos; es decir, en todos los supuestos fácticos previstos en el numeral 217 bis del CP, necesariamente existirá, no sólo un uso indebido de datos, sino, además, una influencia en el sistema automatizado de datos, convirtiéndose este, en el objeto de la acción delictiva.

8. Según lo investigado, la reforma del artículo 217 bis del CP en el año 2012, no era necesaria puesto que ya en nuestro país se contaba con el delito de fraude informático, el cual sancionaba el uso indebido de datos, modalidad de comisión que es la más frecuente, razón por la cual, los fundamentos utilizados por las personas legisladoras, visibilizadas en la investigación, que sirvieron para la construcción del tipo penal de estafa informática no obedecieron a una necesidad social por sancionar una conducta que se encontraba despenalizada, para muestra de ello, la resolución del TASPIICJSJ, N° 587-2016 de las 09:20 horas del 22 de abril de 2016, analizada en el presente trabajo.

9. El delito de estafa informática fue construido como una especie de “Frankenstein” legislativo, ya que, no sólo es un tipo penal abierto, sino que al mismo tiempo es de resultado y de peligro, pero además, es de peligro abstracto y de peligro concreto, lo que permite un amplio margen de discrecionalidad por parte del operador del derecho[342], por lo que se

[342] FERRAJOLI, Luigi. *El paradigma garantista. Filosofía crítica del derecho penal*. Editorial Trotta, S.A., Madrid, 2018, p. 30: *“Lamentablemente, es preciso reconocer que el modelo aquí ilustrado de la jurisdicción como actividad cognoscitiva de aplicación de la ley es un modelo teórico (y normativo), refutado (y violado), de hecho, por los extensos espacios de discrecionalidad que genera el déficit de garantías existente en nuestro sistema judicial: por la carencia de garantías*

considera que, atendiendo principios constitucionales, convencionales y garantistas, deberá entenderse como un delito de resultado, en el cual exista la posibilidad de aplicar el dispositivo amplificador de la tentativa. Esas imprecisiones en la redacción del tipo penal 217 bis del CP, además, lo convierten en pluriofensivo, permitiendo valorar otro tipo de perjuicios que no sean necesariamente de índole patrimonial, en consecuencia, subsiste un problema de concurso aparente de delitos con otras delincuencias, indistintamente que sean de carácter informático, los cuales deben ser valorados casuísticamente.

10. En los supuestos de pesca de datos, si bien en muchos casos éstos son entregados por la víctima al sujeto activo viéndose inducido a error mediante engaño, lo cierto es que, para ese momento todavía no existe una disposición patrimonial, razón por la cual, se descarta el delito de estafa general; y en cuanto al delito de estafa informática, hay que esperar a que el agente haga uso de esos datos sin el consentimiento de quien válidamente lo puede otorgar, ya que de no usarlos, no configuraría los elementos objetivos del tipo penal, en tanto según la redacción de la "estafa" informática es irrelevante el modo de cómo el sujeto activo se haga del conocimiento de datos de la persona agraviada.

11. La praxis judicial refleja que, resulta difícil identificar al imputado que en el ciberespacio o mediante una llamada telefónica, engaña a una persona para obtener sus datos bancarios, sin embargo, como una circunstancia lógica, los dineros de la persona agraviada o entidad bancaria que son sustraídos mediante el uso indebido de datos, necesariamente tendrán que ingresar en otra cuenta destino y posteriormente, esos fondos son retirados o trasladados de una cuenta a otra, es decir, ya sea el titular de la cuenta destino o quien retira el dinero del cajero automático, terminan siendo las caras visibles del delito, quienes serían cómplices o coautores de un delito

---

penales, a causa de la inflación legislativa y la indeterminación semántica de los tipos delictivos, que han abierto espacios incontrolables de discrecionalidad para la intervención penal, en contradicción con el principio de estricta legalidad..."

de estafa informática, dependiendo las circunstancias de cada caso. Del análisis jurisprudencial realizado, se logra concluir que esas son las personas que logra capturar el sistema penal y procesarlos, no así a quienes en principio estaba destinada la creación del delito de “estafa” informática, es decir, las que influyen directamente en el sistema.

12. Existe una falta de claridad acerca de quién debe ser la parte ofendida en los delitos de estafa informática, ello en los supuestos en los que los dineros fueron sustraídos de una cuenta bancaria perteneciente a una persona ya sea física o jurídica, concluyendo mi investigación que en esos casos, no se debe descartar como agraviada la misma entidad bancaria, puesto que es ella en la cual se confía para que custodie los fondos de las personas, es decir, por un tema de seguridad informática, las entidades bancarias podrían ser por un lado víctimas y por el otro, responsables objetivamente hablando por ser quienes resguardan los dineros de las personas ciudadanas. En la práctica, se suele considerar como víctima, únicamente la persona física titular de la cuenta desde la cual se sustraen los fondos, si bien es cierto, ello no es erróneo, no descarta que se aperciba a la entidad bancaria para que manifieste interés en apersonarse al proceso penal.

13. En cuanto a las discusiones generadas en la Asamblea Legislativa que dieron origen al delito de estafa informática, reflejadas en el proyecto de ley tramitado bajo el expediente N.º 17.613, denominado finalmente como: *“Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal”*, se denotó que no existió un abordaje correcto desde un punto de vista jurídico-penal, por ejemplo, no quedaron claros los motivos por los cuales fue necesario modificar el numeral 217 bis del CP que sancionaba el delito de fraude informático; en tanto se argumentó que dicha redacción era útil para zanjar el tema relacionado con el uso indebido de una tarjeta, posición que además había sido legitimada por la jurisprudencia nacional de la STCSJ,

cuando definió que una tarjeta bancaria se igualaba al concepto de llave, ello con la finalidad de tipificar las conductas en el delito de hurto agravado[343], tesis que no comparto, ya que recurre a una apreciación analógica *in malam partem*, ejercicio proscrito en nuestra legislación por el principio de legalidad (artículo 2 del CPP) y su derivado subprincipio de *lex stricta*.

14. Después de realizado el trabajo, no se logra desprender que en las discusiones legislativas existiera algún aporte relevante que determinara el motivo por el cual el delito de estafa informática se tenía que bautizar como una estafa, incluso contrario a lo que posteriormente sugirió el Convenio sobre Ciberdelincuencia desarrollado en Budapest el 23 de noviembre de 2001 (con entrada en vigencia el 01 de julio de 2004), al cual se adhirió Costa Rica mediante la Ley N° 9452 del 26 de mayo de 2017 con entrada en vigencia el 01 de enero de 2018, el cual instaba a regular el "fraude informático". Podría afirmarse que existió influencia del derecho penal español en las personas legisladoras costarricense cuando decidieron denominar el delito como una especie de estafa e insertarle el verbo manipular, pero es que tal y como se estudió, el contenido del delito de estafa regulado en el inciso 2.a del artículo 248 del Código de España, es distinto al nuestro; inclusive, el hecho de que Alemania denomine estafa informática el delito previsto en el artículo §263a del CP de ese país, no quiere decir que nosotros tengamos que llamarlo de esa misma manera; el uso del lenguaje es fundamental para la accesibilidad a la justicia y para hacer el derecho comprensible a las personas usuarias. De *lege ferenda*, se propone que se modifique la nomenclatura del artículo 217 bis del CP y se contemple como único bien jurídico a proteger el patrimonio, con la finalidad de evitar las confusiones que provoca la redacción actual.

15. A nuestro criterio, resultó innecesario bautizar el numeral 217 bis del CP, como una especie de estafa modernizada, al hacerlo, no se obtuvo ningún

[343] Sala Tercera, voto N.º 2006-763 del 18 de agosto de 2006 al ser las 09:20 horas (José Manuel Arroyo, Jesús Ramírez, Alfonso Cháves, Rodrigo Castro y Magda Pereira).

provecho, sino todo lo contrario, se creó confusión y al mismo tiempo, como un efecto punitivo, sancionar con penas de prisión altas, lo que es básicamente el uso indebido de datos. Contradictoriamente los promotores del proyecto legislativo, terminaron "protegiendo" más el medio tecnológico utilizado por el sujeto activo para lesionar el patrimonio, que un ser humano inducido a error mediante engaño a quien le lesionan el patrimonio, siendo éste último supuesto sin lugar a dudas más odioso y reprochable que el primero, más si tomamos en cuenta que el Derecho Penal gira en torno a personas físicas[344].

16. Si comparamos a Costa Rica con los países de Alemania, Argentina y España, tenemos una pena prevista en abstracto mucho más elevada que ellos, la cual oscila entre los 3 y 10 años de prisión; mientras tanto, en Alemania en el artículo §263a del CP, se sanciona con pena de *"hasta cinco años o con multa"*; en Argentina el artículo 173 del CP, prevé una pena tanto para el fraude informático como para el uso indebido de datos de 1 mes a 6 años de prisión; y en España, artículo 248 del CP, dispone en abstracto la pena de prisión de 6 meses a 3 años.

17. En cuanto al aspecto empírico relacionado con la jurisprudencia de los años 2014 al 2019 (inclusive), se evidenció poco aporte sobre el tema por parte de la STCSJ, nótese que se obtuvieron un total de veintiún resoluciones durante ese periodo, es decir, un promedio de 3,5 resoluciones por año, lo cual *prima facie*, demuestra que el tema ha sido poco abordado por dicha Sala de lo penal, ello a pesar de que el tipo penal de estafa informática entró en vigencia desde el año 2012. Ahora bien, dentro de esa cantidad de resoluciones, el tópico de estudio no se analizó a fondo, ya que trece de esas resoluciones se refieren a pronunciamientos sobre admisibilidad de los recursos interpuestos; y cinco resoluciones abordaron conflictos de

[344] FERRAJOLI, Luigi. *El paradigma garantista. Filosofía crítica del derecho penal*. Editorial Trotta, S.A., Madrid, 2018, p. 30: *"El derecho penal mínimo queda entonces caracterizado como la ley del más débil, que en el momento del delito es la parte ofendida, en el del proceso es el imputado y en el de la pena es el condenado..."*

competencia. Las pocas resoluciones que sí hicieron análisis del delito de estafa informática, demuestran una confusión de la STCSJ entre el verbo manipular con el de influir; en otras ocasiones a pesar de estar ante una estafa informática se le trata como fraude informático; e incluso no ha identificado que en realidad el verbo típico es el uso de datos, de modo que se influya en el sistema automatizado de datos.

18. Por su parte, el TASPIICJSJ, si bien durante el mismo lapso, emitió mayor cantidad de resoluciones en comparación a la Sala Tercera, los análisis de fondo con respecto al tipo penal fueron laxos, por ejemplo: Cuando media engaño al momento de obtener los datos de la víctima y utilizarlos, no se ha hecho un análisis profundo de si nos encontramos ante la estafa general del 216 del CP o de la estafa informática; de igual manera, en varias de las resoluciones hizo eco de las resoluciones de la Sala Tercera, arrastrando los errores ya expuestos.

19. A nivel internacional e incluso nacional, siguiendo un sistema meramente capitalista, se ha mencionado que el bien jurídico tutelado de la estafa informática es indiscutiblemente el patrimonio, sin embargo, en nuestro entorno ello no es del todo cierto, puesto que, atendiendo el principio de estricta legalidad, se dejó abierta la posibilidad de lesionar otros bienes jurídicos tutelados.

Es indudable que el delito de la estafa informática tiene muchas aristas que merecen ser estudiadas, por ejemplo: el problema de delimitar el lugar de comisión del hecho y en dónde se produjo o debió producirse el resultado; aspectos concursales con otros delitos; temas relacionados con la tentativa; responsabilidad civil de las entidades bancarias; cuestiones relacionadas con autoría y participación; cómputo de prescripción; así como otros aspectos visibilizados dentro de la investigación, los cuales por lo novedoso de la delincuencia y los usos de la tecnología, han implicado retos importantes para las personas que operan el derecho así como para la misma academia; incluso, como una limitación en el presente trabajo es que a nivel nacional no se cuenta con

bastantes fuentes bibliográficas que hayan analizado extremos puntuales de la estafa informática, como los ya indicados, que sin lugar a dudas merecen ser objeto de futuras investigaciones.

Considero que en la presente tesis se alcanzaron los objetivos propuestos, circunstancia que no obsta que éste trabajo sea cuestionado y debatido, más bien, ello es parte del interés que tuve al realizar la investigación, promover la dogmática penal, siendo que esas discusiones generen conocimiento en las personas interesadas en el tema, de manera que se pretenda evitar la imprevisibilidad en la resolución de los casos procesados bajo este tipo penal.

Para finalizar, es fundamental crear una conciencia social en cuanto a que el derecho no es únicamente para las personas de profesión abogadas, siendo que quienes recurren al sistema judicial (usuarias y usuarios), son las personas que realmente deben tener acceso a la justicia, es decir, se les debe facilitar que puedan comprender sin mayor dificultad conceptos jurídicos, extremo que la estafa informática no cumple; blindar el lenguaje jurídico para hacerlo ininteligible o confuso a las personas usuarias, termina siendo un obstáculo para la accesibilidad a la justicia.

"Nadie puede alegar ignorancia de la ley", establece el artículo 129 de la Constitución Política, frase frecuentemente usada y que se convierte en otra paradoja cuando observamos que quienes son responsables de redactar un delito, lo hacen sin contar con los debidos conocimientos jurídico-penales, no digo que las conductas descritas en el 217 bis del CP no deban ser consideradas dentro del derecho penal, lo que digo es que, el ejercicio de legislar debe cumplir con los subprincipios de *lex certa* y *lex stricta*, los cuales derivan del principio de legalidad; con la estafa informática se creó un tipo penal abierto; sin armonía dentro del contexto del Código Penal, ya que se le denomina estafa sin serlo y está precedido del delito de estelionato (art. 217 del CP); a pesar de que debería, no guarda relación con la estafa convencional del 216 del CP; prevé una pena que no guarda coherencia con la estafa general; no hace diferencia con respecto al tema de la cuantía de lo defraudado; su forma de comisión agravada es más frecuente

que la simple; y por último, fue creado sin hacer una análisis adecuado de cuál era la necesidad de su existencia.

Esperando haber generado y coadyuvado en el conocimiento jurídico costarricense, invito a las personas que estén interesadas en los delitos informáticos a escribir sobre el tema.

Bibliografía

ABOSO, Gustavo Eduardo. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editoriales: Euros Editores S.R.L y Editorial BdeF Ltda., Montevideo, Buenos Aires, 2017.

ANTILLÓN MONTEALEGRE, Walter. *El discurso de la seguridad ciudadana en las recientes reformas procesales*. En: Reflexiones jurídicas frente al populismo penal en Costa Rica. Editorial Investigaciones Jurídicas S.A., 1ª ed. San José, 2012, pp. 19-32.

BALMACEDA HOYOS, Gustavo. *El delito de estafa informática en el derecho europeo continental*. En: Revista de Derecho y Ciencias Penales Nº 17, Chile, 2011, pp. 111-149. Versión electrónica en: https://dialnet.unirioja.es/descarga/articulo/4200389.pdf.

BARRANTES ECHAVARRÍA, Rodrigo*. Investigación: un camino al conocimiento, un enfoque cualitativo, cuantitativo y mixto*. EUNED. 2ª ed. San José, 2016.

BECK, Ulrich. *La sociedad del riesgo*. Traducción de M.ª Rosa Borrás y otros. Editorial Paidós, Barcelona, 1ª ed. 2019.

BECK, Ulrich. *La sociedad del riesgo. Hacia una nueva modernidad*. Traducción de M.ª Rosa Borrás y otros. Editorial Paidós Ibérica, S.A., Barcelona, 1998.

BÉHAR QUIÑONES, Gastón y YÁÑEZ FIGUEROA, Agustín. *Introducción a los contratos tecnológicos*. Editorial Tecnológica de Costa Rica, 1ª ed. Cartago, 2017.

CABANELLAS DE LAS CUEVAS, Guillermo. *Propiedad intelectual sobre los programas de computación*. Heliasta, 1ª ed. Buenos Aires, 2011.

CABALLENAS DE TORRES, Guillermo. *Diccionario de Ciencias Jurídicas*. Editorial Heliasta, 2ª ed. Buenos Aires, 2012.

CASADO, Laura. *Diccionario de sinónimos jurídicos*. Editorial Valleta, 2ª ed. Buenos Aires, 2004.

CASTILLO GONZÁLEZ, Francisco. *El delito de estafa*. Editorial Jurídica Continental, San José, 2ª ed. 2013.

CASTILLO GONZÁLEZ, Francisco. *La estafa informática*. Editorial Jurídica Continental, San José, 1ª ed. 2016.

CASTILLO GONZÁLEZ, Francisco. *La estafa informática de "Lege lata" y de "lege ferenda"*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., pp. 271-313.

CALDERÓN CAMPOS, Marta Eunice. *Marco jurídico de la profesión informática en Costa Rica*. Editorial Universidad de Costa Rica., Costa Rica, 1ª ed. 2018.

CALDERÓN CHINCHILLA, Rosaura. *Crímenes de odio*. En: Delfino. En: https://delfino.cr/2019/06/crimenes-de-odio/, 05-06-2019.

CALDERÓN CHINCHILLA, Rosaura. *El principio de legalidad ¿muro de contención o límite difuso para la interpretación de la teoría del delito en C.R.?* Editorial Investigaciones Jurídicas S.A., 2ª ed. San José, 2018.

CALDERON CHINCHILLA, Rosaura. *Exposición en Seminario sobre Teoría del Delito*. Colegio de Abogadas y Abogados de Costa Rica. En: https://youtu.be/I4pINwyHRU4.

CEDANO OLVERA, Marco Alfredo; CEDANO RODRÍGUEZ, José Antonio; RUBIO GONZÁLEZ, José Antonio; y VEGA GUTIÉRREZ, Arlem Carolina. *Fundamentos de computación para ingenieros*. Grupo editorial Patria, 1ª ed. México, 2010.

CHINCHILLA SANDÍ, Carlos. *Delitos informáticos: Elementos básicos para identificarlos y su aplicación*. Ediciones Farben, 1ª ed. San José, 2004.

CHIRINO SÁNCHEZ, Alfredo y HASSEMER, Winfried. *El derecho a la autodeterminación informativa y el reto del procesamiento automatizado de datos personales*. Editores del Puerto, 1997.

CHIRINO SÁNCHEZ, Alfredo. *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica.* CONAMAJ, San José, 1997.

CHIRINO SÁNCHEZ, Alfredo. *Las tecnologías de la información y el proceso penal*. En: Nexos Costa Rica, Derecho y Legislación. Versión electrónica en: https://www.nexos.co.cr/archivo/perspectivas/tecnologias-informacion-proceso-penal.htm.

CHIRINO SÁNCHEZ, Alfredo. *Las tecnologías de la información y el Proceso Penal. Análisis de una crisis anunciada*. En: Revista de la Asociación de Ciencias Penales de Costa Rica., año 9, n° 14, San José, 1997, pp. 41-53.

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE. *Estado de la banda ancha en América Latina y el Caribe 2016*. Naciones Unidas, CEPAL, cooperación alemana, 2016. Versión electrónica en: https://repositorio.cepal.org/bitstream/handle/11362/40528/6/S1601049_es.pdf.

DONNA, Edgardo Alberto y DE LA FUENTE, Javier Esteban. *Aspectos generales del tipo penal de estafa*. En: Revista Latinoamericana de Derecho, año I, N° 1, 2004, pp. 39-92.

FERNÁNDEZ MORA, Christian. *La racionalidad tecnológica de la justicia penal en Costa Rica y su (Des) Humanización*. En: Revista Digital de la Maestría en Ciencias Penales de Universidad de Costa Rica. Homenaje al Prof. Dr. Francisco Castillo González en sus 70 años. N° 5, ISSN: 1659-4479, 2014, pp. 113-133.

FERRAJOLI, Luigi. *El paradigma garantista. Filosofía crítica del derecho penal*. Editorial Trotta, S.A., Madrid, 2018.

FROSINI, Vittorio. *Cibernética, Derecho, Internet y Sociedad*. Ediciones Olejnik, Santiago-Chile, 1ª ed. 2019.

F(X) FUNCIONES.XYZ en: https://www.funciones.xyz/funcion-identidad/. Consulta realizada el 27 de julio del 2021.

G. SALT, Marcos. *Delitos informáticos de carácter económico.* En revista: Delitos no convencionales. Editores del Puerto s.r.l, Buenos Aires, 1994, pp. 225-249.

GARCÍA FIGUEROA, Alfonso; GASCÓN ABELLÁN, Marina; MARCILLA CÓRDOBA, Gema; PRIETO SANCHÍS, LUIS. *Argumentación jurídica*. Tirant lo Blanch. Valencia. 2014.

GONZÁLEZ AGUDELO, Gloria. *Falsedades*. En: Lecciones de derecho penal: Delitos contra la colectividad, las administraciones públicas y los valores constitucionales. Tomo IV. Editorial Jurídica Continental, 2ª ed. San José, 2017, pp. 161-195.

GONZÁLEZ RUS, Juan José. *Protección Penal de Sistemas, Elementos, Datos, Documentos y Programas Informáticos*. En: Revista Electrónica de Ciencia Penal y Criminología, RECPC 01-14 (1999), ISSN 1695-0194. Madrid, 1999. En: http://criminet.ugr.es/recpc/recpc_01-14.html.

GUERRERO BARRANTES, Elízabeth y SALAZAR RODRÍGUEZ, Alonso. *Comentarios críticos a la reforma del CP que introduce la ley 9048 (sobre delitos informáticos en el derecho penal costarricense)*. En: Revista Judicial, N° 112, Costa Rica, 2014, pp. 247-257.

HARARI, Yuval Noah. *Sapiens. De animales a dioses*. Traducción de Joandomènec. Editorial Penguin Random House, 5ta ed. Barcelona, 2017.

HERNÁNDEZ BASUALDO, Héctor. *Uso indebido de tarjetas falsificadas o sustraídas y de sus claves*. En: Revista electrónica Política Criminal, Nº 5, A2-5,

Chile, 2008. pp. 1-38. Versión digital en: http://politcrim.com/wp-content/uploads/2019/04/A_2_5.pdf.

JAVATO MARTÍN, Antonio Mª. *Sobre: "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"*. En: Revista Electrónica de Ciencia Penal y Criminología. N° 10-r5, ISSN 1695-0194, Valladolid, 2008. Versión electrónica en: http://criminet.ugr.es/recpc/10/recpc10-r5.pdf.

LA NACIÓN. *"Denuncias por fraudes electrónicos en la banca crecieron 36% hasta octubre de 2020"*. Consulta realizada el 23 de noviembre de 2020, en sitio web: https://www.nacion.com/economia/banca/denuncias-por-fraudes-electronicos-en-la-banca/IOXOM53RM5E35DK5LQ5NIM34XI/story/ .

LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 1ª ed. San José, 2011.

LEMAÎTRE PICADO, Roberto. *Manual sobre delitos informáticos para la cibersociedad costarricense*. Editorial Investigaciones Jurídicas S.A., 2ª ed. San José, 2020.

LUZ CLARA, Bibiana. *Manuel de derecho informático*. Editorial Jurídica NOVA TESIS, Argentina, 2001.

MONGE GÓMEZ, Marco. *Cajeros automáticos ¿amigos o enemigos?* En: Revista investigación y ciencia. Organismo de Investigación Judicial, 2ª ed. ISSN 2215-2547. Versión electrónica en: https://sitiooij.poder-judicial.go.cr/index.php/comunicacion/publicaciones/revistas-investigacion-y-ciencia-edicion/item/6691-revista-investigacion-y-ciencia-edicion-n-2, 2012, pp. 5 y 6.

MÜLLER DELGADO, Martha Virginia. *Guía para la elaboración de tesis y consultorio gramatical*. Editorial UCR, 1ª edición revisada, San José, 2015.

ORGANISMO DE INVESTIGACIÓN JUDICIAL. SECCIÓN DE DELITOS INFORMÁTICOS. *Folleto delitos informáticos*. Versión electrónica en: https://sitiooij.poder-judicial.go.cr/images/folletos/delitos%20informaticos.pdf.

OXMAN, Nicolás. *Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"*. En: Revista de Derecho de la Pontificia Universidad Católica de Valparaíso N° 41, Valparaíso. Versión electrónica en: http://www.scielo.cl/scielo.php?pid=S0718-68512013000200007&script=sci_arttext, 2013.

PAREDES CASTAÑÓN, José Manuel. *Vademécum del legislador racional (y decente): Noventa reglas para una buena praxis legislativa en materia penal.* En: Libro-Homenaje a Claus Roxin. Editorial Talleres Gráficos Iustitia, 1ª ed. Perú, 2018, pp. 177-237.

PRESIDENCIA DE LA REPÚBLICA DE COSTA RICA. *En nueve años tarjetas de crédito aumentaron un 125%*. Comunicado del 13-03-2019. En: https://presidencia.go.cr/comunicados/2019/03/en-nueve-anos-tarjetas-de-credito-aumentaron-un-125.

PRESIDENCIA DE LA REPÚBLICA DE COSTA RICA. MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO. *Cuarto estudio trimestral de tarjetas de crédito y débito 2018*. En: http://reventazon.meic.go.cr/informacion/estudios/2018/tarjetas/octubre/pcp.pdf.

PRESIDENCIA DE LA REPÚBLICA DE COSTA RICA. MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO. *Cuarto estudio trimestral de tarjetas de crédito y débito 2019*. En: http://reventazon.meic.go.cr/informacion/estudios/2019/tarjetas/octubre/pcp.pdf.

PRESIDENCIA DE LA REPÚBLICA DE COSTA RICA. MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO. *Primer estudio trimestral de tarjetas de crédito y débito 2020*. En: http://reventazon.meic.go.cr/informacion/estudios/2020/tarjetas/enero/ppc.pdf.

PROGRAMA TELEVISIVO ESPAÑOL “REDES” (dirigido por Eduard Punset) episodio denominado: *"Conciencia y Universo, más allá de la física cuántica"*. En dirección electrónica: https://youtu.be/_7YVlYt5lKo, 2006.

R. PASTOR, Daniel. *¿Es conveniente la aplicación del proceso penal “convencional” a los delitos no “convencionales”?* En revista: Delitos no convencionales, Editores del Puerto s.r.l., Buenos Aires, 1994, pp. 269-301.

ROJAS SALAS, Manuel. *El concepto de perjuicio patrimonial en tipos penales que protegen el patrimonio*. En: Memoria: Ciencias Penales y Derechos Humanos. Homenaje al Profesor Dr. Javier Llobet Rodríguez, San José, Editorial Jurídica Continental, 1ª ed. 2020., pp. 561-581.

S. MARTÍNEZ, Matilde. *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil*. En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, pp.33-47.

SAIN, Gustavo. *La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas más allá de la solución penal*. En compilación:

Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, pp. 7-32.

SALAS PORRAS, Ricardo. *Derecho penal especial*. Editorial Investigaciones Jurídicas S.A, 1ª ed. San José, 2019.

SALINERO ALONSO, Carmen. *Delitos contra el patrimonio (III). Defraudaciones: Estafa. Apropiación indebida. Defraudaciones de fluido eléctrico y análogas*. En: Lecciones de derecho penal: delitos contra la vida, las personas y el patrimonio, parte especial. Tomo III. Editorial Jurídica Continental, 2ª ed. San José, 2017, pp. 503-543.

SÁNCHEZ DELGADO, Daniel. *La estafa. Análisis de sus elementos y problemática con los llamados delitos informáticos*. En: Revista Judicial. Tomo I. Año XX. N° 65, San José, 1997.

SANCHIS CRESPO, Carolina y VELASCO NÚÑEZ, Eloy. *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*. Editorial Tirant lo Blanch, Valencia, 2019.

SUPERINTENDENCIA DE TELECOMUNICACIONES. *Estadísticas del sector de telecomunicaciones,* 1ª edición digital, San José, 2019. Versión electrónica en: https://sutel.go.cr/sites/default/files/informe_estadisticas_del_sector_de_las_telecomunicaciones_2018_vf.pdf.

SUPERINTENDENCIA DE TELECOMUNICACIONES. *Costa Rica con mayor cantidad de hogares con acceso a internet en la región*. Versión electrónica en: https://sutel.go.cr/noticias/comunicados-de-prensa/costa-rica-con-mayor-cantidad-de-hogares-con-acceso-internet-en-la., 2016.

TEMPERINI, Marcelo. *Delitos informáticos y cibercrimen: Alcances, conceptos y características.* En compilación: Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Erreius, 1ª ed. Ciudad Autónoma de Buenos Aires, 2018, pp. 49-68.

ULATE SOTO, Ileana y VARGAS MORÚA, Elizarda. *Metodología para elaborar una tesis*. EUNED. 1ª ed. San José, 2016

Legislación:

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. *Expediente legislativo N° 17.613 del proyecto de ley N° 9048 del 10 de julio de 2012, titulado: "Reforma de varios artículos y modificación de la Sección VIII, denominada delitos*

informáticos y conexos, del Título VII del Código Penal", publicada en el Alcance N.º 172 de La Gaceta N.º 214 del 06 de noviembre de 2012.

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA. *Expediente legislativo del proyecto de ley N° 9135 del 24 de abril de 2013, titulada: "Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal"*, publicada en el Alcance N° 78, de La Gaceta N° 80, del 26 de abril de 2013.

CÓDIGO PENAL DE ALEMANIA.

CÓDIGO PENAL DE ARGENTINA.

CÓDIGO PENAL DE COSTA RICA. Ed. 27. San José, Costa Rica. Editorial Investigaciones Jurídicas S.A., agosto, 2020.

CÓDIGO PROCESAL PENAL DE COSTA RICA. Ed. 16. San José, Costa Rica, Editorial Investigaciones Jurídicas S.A., enero, 2021.

CÓDIGO PENAL DE ESPAÑA.

CONVENIO SOBRE LA CIBERDELINCUENCIA, desarrollado en Budapest, el 23 de noviembre de 2001, con entrada en vigencia el 01 de julio de 2004.

LEY N° 8148 DE 24 DE OCTUBRE DEL 2001, denominada*: Adición de los Artículos 196 bis, 217 bis y 229 bis, al Código Penal Ley N° 4573, para reprimir y sancionar los delitos informáticos*. Publicada en La Gaceta de 21 de noviembre de 2001.

LEY N° 8968 DE *"PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES"*, del 07-07-2011, publicada en La Gaceta N° 170 del 05-09-2011

LEY N° 9452 DEL 26-05-2017, publicada en el Alcance N° 171 de La Gaceta Digital N° 125 del 03-07-2017, con entrada en vigencia el 01-01-2018. Adhesión de Costa Rica al Convenio sobre la Ciberdelincuencia, desarrollado en Budapest, el 23 de noviembre de 2001.

LEY N° 9048 DEL 10 DE JULIO DE 2012, titulada: *"Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal"*, publicada en el Alcance N.º 172 de La Gaceta N.º 214 del 06 de noviembre de 2012.

Jurisprudencia:

Resoluciones Sala Constitucional de la Corte Suprema de Justicia:

N° 1877-90 de las 16:02 h del 19-12-1990.

N° 0447-91 de las 15:30 h del 21-02-1991.

N° 0490-94 de las 16:15 h del 25-01-1994.

N° 9249-2000 de las 15:13 h del 18-10-2000.

N° 11524-2000 de las 14:48 h del 21-12-2000.

N.º 00992-2011 de las 15:47 h del 26-01-2011.

N° 01779-2013 de las 09:05 h del 08-02-2013.

N° 03192-2014 de las 09:05 h del 07-03-2014.

N° 18952-2014 de las 09:05 h del 21-11-2014.

N° 07357-2015 de las 09:15 h del 22-05-2015.

Resoluciones de la Sala Tercera de la Corte Suprema de Justicia:

N° 2012-00032 de las 10:07 horas del 13-01-2012.

N° 2006-00148 de las 09:00 horas del 24-02-2006.

Nº 2014-00616 de las 09:05 horas del 04-04-2014.

Nº 2014-01322 de las 10:02 horas del 01-08-2014.

Nº 2014-01563 de las 13:11 horas del 29-09-2014.

Nº 2014-01669 de las 09:48 horas del 17-10-2014.

Nº 2014-01783 de las 15:45 horas del 10-11-2014.

Nº 2014-01909 de las 11:38 horas del 10-12-2014.

N° 2015-00354 de las 09:55 horas del 27-02-2015.

N° 2015-00788 de las 11:02 horas del 24-06-2015.

Nº 2015-01292 de las 09:28 horas del 16-10-2015.

Nº 2015-01370 de las 08:52 horas del 06-11-2015.

Nº 2016-00887 de las 09:39 horas del 09-09-2016.

Nº 2016-01025 de las 14:32 horas del 29-09-2016.

Nº 2016-01081 de las 09:59 horas del 14-10-2016.

Nº 2016-01241 de las 10:15 horas del 02-12-2016.

Nº 2017-01097 de las 11:28 horas del 15-12-2017.

Nº 2018-0464 de las 16:25 horas del 20-06-2018.

Nº 2018-0597 de las 10:32 horas del 31-08-2018.

Nº 2018-00639 de las 09:57 horas del 14-09-2018.

Nº 2019-00498 de las 18:45 horas del 25-04-2019.

Nº 2019-001501 de las 11:30 horas del 22-11-2019.

Nº 2019-001591 de las 10:27 horas del 13-12-2019.

Resoluciones del Tribunal de Apelaciones de la Sentencia Penal del II Circuito Judicial de San José:

N° 0521-2014 de las 11:00 horas del 19-03-2014.

N° 0600-2014 de las 13:22 horas del 28-03-2014.

N° 1244-2014 de las 09:00 horas del 11-07-2014.

N° 1413-2014 de las 10:20 horas del 05-08-2014.

N° 1542-2014 de las 16:20 horas del 21-08-2014.

N° 1727-2014 de las 11:53 horas del 05-09-2014.

N° 1732-2014 de las 14:32 horas del 05-09-2014.

N° 2030-2014 de las 10:00 horas del 15-10-2014.

N° 2037-2014 de las 14:07 horas del 16-10-2014.

N° 2097-2014 de las 15:45 horas del 23-10-2014.

N° 2315-2014 de las 10:15 horas del 28-11-2014.

N° 2433-2014 de las 15:10 horas del 17-12-2014.

N° 0230-2015 de las 11:05 horas del 13-02-2015.

N° 0323-2015 de las 11:20 horas del 02-03-2015.

N° 0389-2015 de las 13:55 horas del 13-03-2015.

N° 0436-2015 de las 09:10 horas del 20-03-2015.

N° 0535-2015 de las 17:45 horas del 09-04-2015.

N° 0738-2015 de las 09:05 horas del 22-05-2015.

N° 0844-2015 de las 14:50 horas del 11-06-2015.

N° 0917-2015 de las 15:20 horas del 25-06-2015.

N° 1157-2015 de las 15:45 horas del 19-08-2015.

N° 1425-2015 de las 16:00 horas del 22-10-2015.

N° 0225-2016 de las 11:10 horas del 15-02-2016.

N° 0450-2016 de las 14:15 horas del 28-03-2016.

N° 0480-2016 de las 14:20 horas del 30-03-2016.

N° 0587-2016 de las 09:20 h del 22-04-2016.

N° 0690-2016 de las 15:30 h del 10-05-2016.

N° 0836-2016 de las 10:20 h del 06-06-2016.

N° 0976-2016 de las 15:05 h del 29-06-2016.

N° 1326-2016 de las 13:40 h del 16-09-2016.

N° 1496-2016 de las 15:15 h del 26-10-2016.

N° 1700-2016 de las 10:35 h del 16-12-2016.

N° 1768-2016 de las 15:00 h del 22-12-2016.

N° 0256-2017 de las 11:00 h del 03-03-2017.

N° 0617-2017 de las 14:20 h del 26-05-2017.

N° 0851-2017 de las 08:52 h del 12-07-2017.

N° 1016-2017 de las 10:45 h del 22-08-2017.

N° 0034-2018 de las 09:00 h del 17-01-2018.

N° 0197-2018 de las 09:30 h del 16-02-2018.

N° 0200-2018 de las 09:05 h del 16-02-2018.

N° 0671-2018 de las 15:00 h del 28-05-2018.

N° 1048-2018 de las 09:55 h del 09-08-2018.

N° 1082-2018 de las 10:25 h del 13-08-2018.

N° 1280-2018 de las 10:35 h del 20-09-2018.

N° 1643-2018 de las 11:25 h del 19-11-2018.

N° 1816-2018 de las 09:20 h del 13-12-2018.

N° 1876-2018 de las 14:20 h del 18-12-2018.

N° 1899-2018 de las 08:20 h del 21-12-2018.

N° 0097-2019 de las 15:20 h del 24-01-2019.

N° 1431-2019 de las 16:10 h del 19-08-2019.

N° 1818-2019 de las 10:05 h del 11-10-2019.