UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

MAESTRÍA EN DERECHO CON ÉNFASIS EN DERECHO PENAL

LA ESPECIFICIDAD DE LA CONFIGURACIÓN TÍPICA DE LOS DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LOS PROCESOS PENALES.

JOSÉ BENJAMÍN HIDALGO DURÁN

SAN JOSÉ, FEBRERO 2021

CONTENIDO

RESUMEN EJECUTIVO

Con el auge del Internet y las telecomunicaciones, se acrecienta el número de delitos informáticos que se tornan un foco de atención en gran parte del mundo, incluyendo el ámbito costarricense. Es así como, a partir del nacimiento de las tecnologías citadas, surgen novedosos tipos penales con el fin de contrarrestar esta nueva delincuencia.

Para empezar, el objetivo del proyecto investigativo es analizar la especificidad de la configuración típica de los elementos normativos en los tipos penales informáticos de estafa informática, suplantación de identidad y difusión de información falsa. Con este fin, la pregunta de investigación es: ¿Incide la configuración típica de los elementos normativos de los tipos penales informáticos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense, en los resultados de los procesos penales, tomando como referente las resoluciones de la Sala Tercera y los tribunales de apelación de sentencia penal del año 2019 y 2020?

Para obtener la respuesta, se realiza una conceptualización teórica del Internet y la tecnología informática, además de un análisis de las opiniones de expertos y de la jurisprudencia de sentencias.

Desde los parámetros indicados, en el presente trabajo se analiza si la configuración típica de los elementos normativos de los tipos penales informáticos citados, tiene una incidencia directa en los resultados de los procesos penales. A partir de este análisis, se evidencia que existe desconocimiento o bien, ambigüedad en dicha configuración, que se manifiesta desde la presentación de la denuncia ante el Ministerio Público, hasta el desarrollo del proceso en los tribunales. Por tanto, cuando se alude a delitos informáticos, la estafa informática suele ser la más recurrente; esta desencadena dificultades para ubicar al sujeto activo y, a la vez, para presentar

pruebas, porque no hay certeza de los equipos que se han utilizado en cada delito, lo que resulta en impunidad.

Por ende, se necesita más capacitación y presupuesto de quienes conforman el Organismo de Investigación Judicial (OIJ), una formación integral de la Judicatura, para lograr mejoras sustanciales en la persecución del sujeto activo y que Costa Rica cuente con un equipo interdisciplinario dotado de los conocimientos científicos en informática y el equipo idóneo para perseguir de manera integral este tipo de delincuencia.

Palabras clave. **Delito informático, estafa, suplantación, difusión, tipificación.**

CAPÍTULO I: INTRODUCCIÓN

1. Tema

La especificidad de la configuración típica de los delitos informáticos y su incidencia en los procesos penales.

1.1 Planteamiento del problema

¿Incide la configuración típica de los elementos normativos de los tipos penales de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense, en los resultados de los procesos penales, tomando como referente las resoluciones de la Sala Tercera y de los tribunales de apelación de sentencia penal del año 2019 y 2020?

1.2 Objetivos

1.2.1 Objetivo general.

Analizar si la especificidad de la configuración típica de los elementos normativos de los tipos penales informáticos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense, repercute en los resultados de los procesos penales.

1.2.2 Objetivos específicos

1- Indagar, a través de los operadores del proceso penal (personas defensoras públicas/privadas, informáticos, fiscales y jueces), si la configuración típica de los elementos normativos de los tipos penales informáticos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236) todos del Código Penal costarricense, tienen alguna incidencia en los resultados de los procesos penales.

2- Revisar la jurisprudencia de los Tribunales de Apelación de Sentencia y la Sala Tercera del año 2019 y 2020, respecto a los delitos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense, con el fin de identificar si la configuración típica normativa de la citada delincuencia incide en los resultados de los procesos penales.

3- Analizar, desde un abordaje práctico (jurisprudencias analizadas y operadores del sistema entrevistados), la especificidad de la configuración típica normativa de los delitos informáticos (estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense) respecto a la incidencia en los resultados de los procesos penales.

1.3 Justificación

Con el surgimiento del Internet, en los años sesenta, revolucionó la tecnología. El avance y la evolución de la informática favorecen las labores de la población mundial, debido a su agilidad, ya que, el ahorro del tiempo juega un papel importante actualmente.

Gracias a los avances tecnológicos, ahora las personas se pueden comunicar desde cualquier parte del mundo en segundos y, también, realizar todo tipo de transacciones desde la comodidad del hogar o la oficina, lo que ha sido un beneficio. Lo que por un lado resulta de gran ayuda, por otro, origina un panorama que es aprovechado por los piratas informáticos, quienes socavan información confidencial de terceras personas o de sus finanzas, creando con ello una sensación de inseguridad en la población y en las autoridades.

.

Lo anterior ha aumentado la preocupación de las autoridades estatales, dado que un gran sector de la población ha sido afectado por los delincuentes informáticos, los cuales utilizan herramientas tecnológicas para crear un perjuicio en el patrimonio de las personas y existe toda una ingeniería social detrás de este tipo de delincuencia.

Con respecto a esta investigación, se pretende analizar, desde un abordaje práctico (jurisprudencias y operadores del sistema), la especificidad de la configuración típica normativa de los delitos informáticos (estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense) respecto a la incidencia en los resultados de los procesos penales.

Por esa realidad, Mata y Martín (2003) refieren que, en este tipo de comunicación, existen quienes exploran los nuevos medios de las computadoras y las redes con fines delictivos: robo de información, falsas ofertas, sabotaje y espionaje informático, interceptación no autorizada, piratería, estafas de subastas *online,* intrusiones en redes y un sinnúmero de los denominados delitos cibernéticos, ciberdelitos, o cibercrímenes. En ellos, se jaquean permanentemente a personas naturales, instituciones públicas y empresas privadas de todo el mundo.

En una era en que el Internet ha significado nuevos paradigmas en procesos de comunicación de masas, se hizo necesario regular, de diferentes maneras esta materia, especialmente, mediante el derecho penal, el cual, trata las conductas antisociales que se encuentran íntimamente relacionadas con las tendencias tecnológicas.

Cada vez, con mayor frecuencia e impacto, los dispositivos para almacenar y procesar información (servidores, estaciones de trabajo o computadoras personales) son vulnerados en sus componentes más sensibles. Así, se exponen no solo datos específicos e importantes (financieros, crediticios, estratégicos, productivos, entre otros), sino también los patrimonios de personas y

organizaciones y, aún más preocupante, su dignidad, su honra y su vida privada. Por ejemplo, en el caso de Costa Rica, se realizaron modificaciones en la normativa penal relacionadas con la inclusión de tipos delictivos como sabotaje o estafa informática que, desde el año 2001, como se analizará posteriormente, fueron parte de los esfuerzos para responder al auge vertiginoso de la *web*, convertida en terreno fértil para la comisión de hechos delictivos y como zona perfecta para que los delincuentes se oculten.

Ahora bien, en busca de la comprensión de los nuevos paradigmas, la presente investigación afronta tres vertientes: en primera instancia, una revisión amplia de la bibliografía en materia de cibercriminalidad y los tipos penales de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236) todos del Código Penal costarricense. En segundo lugar, se analizan temas conexos desde el conocimiento y la experiencia que poseen algunos operadores del derecho y expertos en informática; se realiza a través de entrevistas a operadores judiciales como a ingenieros informáticos, junto con casos específicos de jurisprudencia en la Sala Tercera y II Circuito Judicial de San José. Por último, se analiza la especificidad de la configuración típica de los delitos informáticos y cómo esta puede incidir en los resultados de procesos penales que tramitan la delincuencia apuntada.

Desde la perspectiva indicada, el presente trabajo de investigación responde a una realidad del país, pues Costa Rica no está exenta del accionar de delincuentes cibernéticos. A diario se está a merced de personas inescrupulosas que cometen delitos con un alto potencial transfronterizo porque, aunque se efectúan en el territorio de un país, sus efectos pueden trascender a otras latitudes transfronterizas.

Adicionalmente, resulta preocupante que, a pesar de la existencia de tipos penales informáticos en la legislación costarricense, todavía se evidencia mucha impunidad que podría

estar asociada a la complejidad y la particularidad típica de los elementos normativos de los tipos penales, estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236) todos del Código Penal costarricense que inciden en los resultados de los procesos penales, donde se investiga la delincuencia señalada. Este tema por su relevancia se retomará más adelante.

Adicional a lo anterior, pareciera ser que existe algún desconocimiento de criterios, técnicas y conceptos asociados a la informática que se encuentran inmersos en la configuración típica de los delitos penales de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense por parte de los operadores del sistema penal, que incide no solo en el desempeño de dichos profesionales, sino también en la suerte de los procesos judiciales.

Por ende, para realizar una adecuada judicialización en materia de ciberdelincuencia, es fundamental el papel de los operadores del derecho, por lo que, mediante esta investigación se pretende conocer si la composición típica normativa de los delitos citados *supra* es un obstáculo que incide tanto en el desempeño técnico de las personas juezas, fiscales y defensores públicos y privados, como en los resultados de los procesos judiciales que tramitan esta delincuencia.

Con la finalidad descrita, se propone analizar las características peculiares típicas objetivas y normativas que presentan los tipos penales mencionados anteriormente, en los resultados de los procesos penales y en el acceso a la justicia.

Finalmente, para efectos del proceso investigativo, se considera el informe realizado por Víctor Fernández, funcionario del Organismo de Investigación Judicial, Oficina de Planes y Operaciones (2020), donde facilita la información de los delitos informáticos denunciados en el periodo que va del 8 de agosto del 2018, al 22 de octubre de 2020, en el que se determina que los

delitos más comunes y de mayor cantidad de denuncias son: estafa informática (artículo 217 bis), suplantación de identidad (artículo 230) y difusión de información falsa.

1.4 Antecedentes

Con respecto a la historia que antecede al tema en estudio, se debe indicar que las primeras acciones delictivas relacionadas al uso de la informática datan de los años sesenta, con la evolución de la industria tecnológica y su desarrollo vertiginoso. Al respecto, Morales Prats (citado en Hernández, 2009), indicaba que:

> (…) la ingente acumulación de datos de carácter personal de la ciudadanía por parte de los gobiernos, aun cuando no estaba masificado el uso de los ordenadores, hace que comiencen las preocupaciones en torno al carácter reservado, la acumulación y el uso que podría hacerse de estos datos (p. 229).

Del mismo modo, agrega Hernández (2009) que, en los años ochenta:

> (…) la generalización de los ordenadores personales entre la población trajo consigo, el surgimiento de la piratería del software. Tempranamente, se mostraron a favor de esta opción de los mismos, dando comienzo así a las primeras infracciones contra la propiedad intelectual que se generalizarían a finales de los años noventa, extendiéndose, además, dicho software, a productos como música o películas (pp. 229-230).

Como se evidencia, la criminalidad informática comienza a moldearse con la ayuda de los adelantos tecnológicos y se constituye como una de las técnicas de delitos más lucrativas y, a la vez, más difíciles de detectar por las autoridades en cada país. Lo anterior debido a que estas actividades se conforman de una gran logística, implementación y ejecución compleja a través de las cuales, personas inescrupulosas socaban el patrimonio de millones de víctimas físicas y jurídicas.

Dentro de los antecedentes de la temática desarrollada, se deben considerar otros autores, entre los que se menciona, primeramente, Albizuri (2002), quien, analiza la problemática referente al fraude y a la delincuencia informática. Además, colabora con la caracterización del fraude informático y los hackers ("entrometidos"), quienes se dedican a perpetrarlos. En su artículo, la autora argumenta y justifica la dificultad en la detección y la prueba del delito informático y finaliza con la propuesta de la necesidad de un código ético y una deontología profesional propia de los informáticos, como la forma más adecuada para evitar el fraude y la delincuencia en ese ámbito y colaborar con el incremento de la seguridad de los sistemas informáticos.

Otra investigación, desarrollada por López y Torres (2010), destaca el enfoque de una perspectiva internacional por el avance del Internet y el problema transfronterizo. Este genera, por un lado, beneficios para los ciudadanos y, por otro, una serie de inconvenientes tanto para las personas inocentes como para las empresas y, por supuesto, para el derecho en general, especialmente el penal, pues, existen vacíos o inconsistencias jurídicas, mucha desprotección para la ciudadanía, tanto de quienes no saben utilizar las herramientas informáticas como de quienes dominan su uso, debido a que no están exentos de ser víctimas de delitos y amenazas cibernéticas.

Con respecto a esta situación que han causado las nuevas tecnologías, los autores citados destacan la importancia de proteger la información contenida en un sistema informático como bien jurídico; sin embargo, a diferencia del trabajo por investigar, se debe desarrollar la especificidad de los delitos informáticos, de ahí la importancia de esta tesis de investigación.

En el ámbito internacional, un antecedente relevante es el de Quevedo (2017). En su investigación, desarrolló varios argumentos, entre los que destaca que la prueba del delito exige la adopción de precauciones especiales para evitar que se frustre la labor investigadora o se vulneren derechos fundamentales. Indica que se estudian cuestiones básicas que suscitan los ciberdelitos

como competencia para conocerlos, donde se destacan los conflictos de jurisdicción entre Estados, la cooperación internacional y los sujetos especializados en la investigación con especial referencia a los Equipos Conjuntos de Investigación, así como a las obligaciones a las que vienen sujetas las empresas proveedoras de Internet.

Un aspecto que se destaca en la propuesta de Quevedo (2017) es la importancia de realizar un análisis de la regulación legal de las medidas de investigación tecnológica necesarias para la investigación del ciberdelito; en concreto, destaca que, en torno a la prueba, la característica es que al ejecutarse su comisión en un ámbito virtual, la demostración del hecho delictivo necesita de elementos físicos, no solo de datos electromagnéticos, por lo que es necesario encontrar los equipos utilizados en la comisión del hecho como material de prueba. Por último, esta investigación abarca desde lo básico de los ciberdelitos hasta la competencia para conocerlos y las diversas dificultades que pueden generar estos tipos de delitos, incluso a nivel internacional, todo esto con base en el soporte tecnológico y sus profesionales.

Si bien las tecnologías digitales han mejorado las condiciones de vida, también se convirtieron en el escenario perfecto para delincuentes que utilizan los avances a su provecho. El presente trabajo de investigación pretende añadir un acápite importantísimo para Costa Rica, al desarrollar la especificidad de tres tipos penales informáticos supra señalados, para conocer de primera mano cómo repercute en la aplicación práctica a nivel de abogados litigantes, defensores públicos y administradores de justicia.

1.4.1 Regulación de la ciberdelincuencia en el ámbito costarricense.

Para responder a los cambios señalados en el apartado precedente, en el ámbito nacional se realizaron modificaciones en el Código Penal, por ejemplo, en la Ley N.º 8148 del 24 de octubre del 2001, se incorporaron los artículos 217 bis y 229 bis, que regulan el fraude y el sabotaje

informático, respectivamente. Estas modificaciones, respondían a la necesidad de reglamentar las conductas que puedan resultar penalmente censurables.

Del mismo modo, la reforma de la sección VIII, Delitos Informáticos y Conexos, del título VII del Código Penal N.º 9048, conocida como la Ley de delitos informáticos, introduce nuevos tipos al Código Penal costarricense vinculados al uso de la tecnología. Posteriormente, se sancionó la Ley N.º 8968 de Protección de la Persona frente al tratamiento de sus datos personales, el 5 de noviembre de 2011, para establecer la facultad que tiene cada individuo de proteger su intimidad y decidir qué datos personales pueden ser o no tratados, almacenados, transferidos, divulgados y comercializados en el territorio de la República de Costa Rica. Todas estas modificaciones surgieron como respuesta a la necesidad cambiante de combatir delitos que, hoy por hoy, van en aumento.

CAPÍTULO II: MARCO TEÓRICO

2.1 Algunos aspectos relacionados con tecnologías de la información, telecomunicaciones y derecho informático

Para el trabajo de investigación, se tiene como primer objetivo indagar a través de los operadores del proceso penal (personas defensoras públicas/privadas, informáticos, fiscales y jueces) si la configuración típica de los elementos normativos de los tipos penales informáticos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense, tienen alguna incidencia en los resultados de los procesos penales. Para esto, es necesario desarrollar algunos aspectos relevantes, específicamente en Costa Rica, de las Tecnologías de la Información y la Comunicación (TIC) y conceptualizar los términos informáticos relacionados y aplicados en los tipos penales.

2.2 Generalidades de la evolución histórica de las TIC a nivel mundial

Las TIC permiten el acceso a videojuegos, mensajes de texto, comercio electrónico, transacciones en entidades estatales, financieras, entre otras. Utilizan plataformas virtuales para que los usuarios puedan agilizar procesos sin salir de su casa o desde cualquier ubicación mediante aparatos móviles. Si bien son herramientas que han facilitado la labor del ser humano, por otra parte, algunas personas han encontrado una oportunidad para utilizarlas en provecho propio y en perjuicio de terceros.

Es por ello que se ha hecho necesario en Costa Rica, así como en otras partes del mundo, tipificar las conductas de los ciberdelincuentes que causen perjuicio a terceras personas; sin embargo, las tecnologías evolucionan de manera muy rápida y las personas siguen teniendo afectaciones en su esfera patrimonial y en su privacidad, en procesos que en su mayoría son

sobreseídos por parte del Ministerio Público. Por ello, esta investigación enfoca sus objetivos en analizar si la especificidad de la configuración típica de los elementos normativos de los tipos penales informáticos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense, repercute en los resultados de los procesos penales.

De igual manera, se indagará a través de los operadores del proceso penal (personas defensoras públicas/privadas, informáticos, fiscales y jueces y se revisará la jurisprudencia de los Tribunales de Apelación de Sentencia y la Sala Tercera del año 2019 y 2020, respecto a los delitos informáticos mencionados.

Ahora bien, es importante tener una conceptualización clara y específica del término TIC. Al respecto, los expertos han dicho lo siguiente:

> (…) es el conjunto de herramientas, soportes y canales desarrollados y sustentados por las tecnologías (telecomunicaciones, informática, programas, computadores e internet) que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos, contenidos en señales de naturaleza acústica, óptica o electromagnética a fin de mejorar la calidad de vida de las personas (Ávila, 2013, pp. 222-223).

Aunque el surgimiento de las TIC ha traído un enorme beneficio al mundo, también muchos retos a los entes de policía en materia de delincuencia. Los datos y el patrimonio de las empresas y las personas han sido, en algunos casos, vulnerados y se facilita la comisión de delitos, como se observará posteriormente.

Estas herramientas tecnológicas evolucionan de manera acelerada y, con el tiempo, sufren una serie de transformaciones, como puntualiza Ávila (2013):

> Se debe hacer notar que las tecnologías de las comunicaciones giran en tres etapas a saber: la primera es la edad del cable, que va desde 1844 a 1900; la segunda va desde 1900 a 1980 y se llama la edad de la transmisión inalámbrica y la tercera es la que se denomina la edad de las redes digitales integradas, cuyo tiempo corresponde entre 1980 hasta la fecha (p. 222).

Para comprender el contexto del crecimiento tecnológicos, se exponen, a modo de resumen, ideas importantes señalabas por Ávila (2013) y su subdivisión en periodos: en la primera etapa, de 1844 a 1900, entre muchas otras situaciones, se perfecciona el código morse, se inventa la línea de larga distancia de transmisión telegráfica, la primera alarma de incendios, el teléfono, la central telefónica, la radiotelegrafía, las antenas. En la segunda etapa, que va del año 1900 a 1980, se da la primera comunicación transoceánica, las antenas evolucionan, se tiene el primer sistema de transmisión de voz, amplificadores de radio frecuencia, la transmisión AM, emisiones diarias de música por radio, memoria binaria, una emisora transmite el primer concierto de música clásica, primera central de telefónica de larga distancia, la televisión, la calidad de video, el sistema radar, los cables coaxiales, la televisión comercial, la calculadora, el casete para grabación, la computadora, la cámara de video electrónica, el satélite de comunicaciones. La IBM introduce el teleprocesamiento, es decir, los datos transmitidos por línea telefónica se reprocesan o reflejan en un computador. Para el año 1980 y hasta el presente, se origina la tecnología de sonido multinacional, *cd player*, discos compactos, telefax, computadoras personales, VHS, DVD, red celular, formatos de audio digital (DAT), televisión de alta definición, televisión por cable, televisión vía móvil, Internet comercial, entre otras cosas.

2.3 Generalidades de la incursión de las tecnologías digitales en Costa Rica

Paulatinamente, la humanidad cambia y, en esa transformación, evoluciona tecnológicamente en aspectos como: la invención de la computadora, los programas, el equipo, los teléfonos celulares, el Internet comercial, las plataformas virtuales, pues ayudan a simplificar la vida de las personas. Costa Rica, no se encuentra ajena a esta evolución.

Respecto a este punto, Jara y Álvarez (2008) manifiestan:

> El desarrollo de la industria de TIC en Costa Rica tiene sus orígenes en la década de los años 70 y la base de ese desarrollo tuvo esencialmente dos cimientos (a) la inversión pública de educación, salud e infraestructura; y (b) el énfasis puesto en la transferencia tecnológica (pp. 2-3).

Se observa que, poco a poco, las TIC incursionan en Costa Rica, lo que se evidencia con la creciente inversión en educación y tecnología que hace el gobierno. Posteriormente, se abren carreras con énfasis en computación, así como ingenierías en esta materia. Además, algunas empresas son pioneras en la dedicación de programas y mantenimiento de computadoras. Con esto, el país tiene un auge importante dentro de la industria de la computación.

> Los principales factores que caracterizaron la industria del software en Costa Rica durante los años noventa se pueden resumir de la siguiente manera:
>
> -Carencia de aplicaciones y demanda natural: en Latinoamérica se da un “boom” de crecimiento en el desarrollo de aplicaciones de buena calidad a mediados de los noventa.
>
> -Demanda sustantiva de aplicaciones por la llegada del nuevo milenio, que incrementó la demanda de aplicaciones que hicieran frente al YK2000.
>
> -Primera oleada de aplicaciones por internet, generando una moda de aplicaciones por este medio, provocando más demanda de productos del sector (Jara & Álvarez, 2008, pp. 4).

De esta forma, Costa Rica evoluciona con las TIC; con ello, se da la llegada de las multinacionales que invierten en temas de computadoras, *software*, *hardware*, mantenimiento, aplicaciones, todo de la mano del Internet comercial y las redes sociales. Sin embargo, como se ha mencionado, las tecnologías de la información y la comunicación son utilizadas por los infractores de la ley para cometer diversidad de delitos. De esta manera, se evidencia que es necesario emplear un abordaje de términos informáticos que se apliquen en los tipos penales, así como conocer y estudiar las técnicas con las que se cometen estos delitos.

2.4 El ciberespacio, la criminalidad y la informática: una mirada desde el sistema penal costarricense

En esta sección, se abarcarán tres conceptos importantes: el ciberespacio, la criminalidad y la informática, los cuales se visualizarán desde una perspectiva del Sistema Penal costarricense. Esto contribuye a contextualizar las definiciones de una mejor manera durante el trabajo investigativo.

En primer lugar, el ciberespacio es la unión entre lo tecnológico a través del Internet con gran cantidad de información virtual; es decir, un espacio no físico, que no tiene límites y donde cualquier persona puede estar conectada a la red e interactuar con muchas personas sin obstáculos.

Sobre la criminalidad informática, Hernández (2009), expone:

> La doctrina quizás hoy mayoritaria prefiere acudir a aquellas expresiones de “delincuencia informática” o “criminalidad informática” para incluir en ellas todos los comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera, y todos aquéllos en que dicho sistema sea él mismo el propio objeto sobre el que recae la acción delictiva (p. 235).

Es así como, con la llegada del ciberespacio y con el advenimiento de nuevas técnicas de delincuencia, los bienes jurídicos como: intimidad, datos personales, seguridad comercial, e inclusive, propiedad intelectual, ameritaron una respuesta penal en Costa Rica, ya que esta clase de delincuencia presume varios cambios en el Código Penal.

Sin embargo, estas reformas sobre delitos informáticos de los últimos años conllevan varios problemas en el campo de la informática de quienes administran justicia. Se debe tener la idoneidad para entender el tipo penal, la prueba y la comprensión del delito informático por parte del juzgador, el fiscal, el defensor, al igual que los investigadores, para poder hacer frente a la criminalidad informática. Al respecto, indica Hess (2010): “En Costa Rica hemos tenido un enfoque, como les decía ahora, completamente confuso e inconsistente con relación al tratamiento de los delitos informáticos y hemos terminado en nuestra legislación con lo que yo llamo una verdadera “ensalada normativa”” (p.130).

Lo indicado por el autor es de suma importancia para esta investigación, pues parte del problema sobre este tipo de delincuencia es precisamente que existe un desorden en la ubicación de los tipos penales dentro del Código Penal. Estos no se encuentran unificados, lo que no solamente crea un problema a los operadores de justicia, sino también a la población en general, quienes bajo el principio de taxatividad y de legalidad tienen el derecho de poder encontrar el tipo penal de delitos informáticos en un solo cuerpo normativo y, además, que sea comprensible para toda la población.

2.4.1 Términos informáticos y técnicas delictivas para cometer cibercrímenes.

Para entender de forma más adecuada el desarrollo, el estudio y el planteamiento del tópico de fondo de esta investigación, se considera necesario conocer la terminología técnica que

compone la tipicidad, especialmente, la objetiva y la normativa de los tipos penales: estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense, así como las técnicas y la manera de comisión de la delincuencia informativa apuntada.

Primeramente, Parker (citado en Hernández, 2009) definió los abusos informáticos como "cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio" (p. 231). Este autor no se limitó a describir las conductas relevantes para el ámbito penal, sino que reconoce que se trata de un amplio abanico de conductas en las que se incluyen las de naturaleza penal, otras de relevancia civil y meros incidentes, sin trascendencia jurídica.

A pesar de la vertiente patrimonial de su estudio, Bequai (citado por Hernández, 2009) se preocupó por los ataques a la intimidad que, con la creación de las primeras bases de datos, podían derivarse al digitalizar la información de naturaleza privada. En este sentido, cabe resaltar que los ordenadores pueden ser usados por el autor del delito, no solo como instrumentos para cometerlo, sino como objeto del delito. Asimismo, dentro de los *computer crimes*, se incluyeron los delitos de sabotaje informático, robo de información digitalizada y programas, espionaje industrial, hurto de tiempo de uso del ordenador, robos de mercancías por manipulación de datos o fraudes financieros.

Dentro de la informática existe diversidad de técnicas para delinquir, con el desarrollo de la tecnología y sus avances; por ende, los criminales también evolucionan y crean mecanismos para cometer ilícitos. Ante esto, algunas instituciones instruyen a sus usuarios sobre la seguridad informática. Un ejemplo es el caso del Banco de Costa Rica, pues en su página principal han formulado un glosario que intenta alertar a sus clientes, indicándoles que los delincuentes utilizan

herramientas tecnológicas para el crimen, donde la entidad bancaria no solamente introduce el nombre de los posibles virus a los que se expone la clientela, sino también su definición.

En ocasiones, los delincuentes informáticos solicitan o indican al usuario, a través de mensaje de texto, que acceda a la página web de la entidad en cuestión, que es una copia idéntica de la original, donde deberá completar dicha información. Actualmente, están surgiendo numerosas versiones de este delito, que se sirven de otro tipo de medios para conseguir los mismos fines.

Con respecto a los virus, las técnicas más conocidas para afectar a los equipos de cómputo son programas en los cuales el delincuente desea alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Generalmente, infectan archivos y el disco duro con la clara intención de modificar o destruir alguna información almacenada en la computadora. Ahora bien, todos los términos anteriores citados son herramientas para cometer los delitos informáticos, los cuales se desarrollan más adelante.

2.5 Análisis de la tipicidad de los delitos informáticos: estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), del Código Penal costarricense, con énfasis en elementos objetivos y normativos

El objetivo general de esta investigación es analizar si la especificidad de la configuración típica de los elementos normativos de los tipos penales informáticos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), del Código Penal costarricense, repercute en los resultados de los procesos penales. De ahí la importancia que tiene para esta investigación definir los términos clave para el área de estudio: *hardware, software, malware,* virus informático, *hacker,* aplicaciones web, comunidades virtuales, para ello, se ofrecen definiciones breves de diferentes autores:

A) *Hardware:* es definido por la RAE como “equipo”, desde el punto del lenguaje técnico se identifica con este término los elementos físicos de la arquitectura de un ordenador, desde la CPU hasta el monitor, pasando por todos los periféricos que pueden ser acoplados al ordenador. (Herrera, 2017, p.4)

B) *Software:* **equipamiento lógico e intangible** de un ordenador. En otras palabras, el concepto de software abarca a todas las **aplicaciones informáticas**, como los procesadores de textos, las planillas de cálculo, los editores de imágenes, los reproductores de audio y los videojuegos, entre otras muchas. (Pérez y Gardey, 2008,parr 2)

C) *Malware* (SITEMAP de tecnología): es el término abreviado que significa "software malicioso". Este es un software (programa) que está diseñado específicamente para obtener acceso o dañar un ordenador sin el conocimiento del propietario. Hoy en día, gran parte del *malware* es creado con fines de lucro a través de publicidad forzada (*adware)*, el robo de información sensible (software espía), la difusión de correo electrónico de spam o pornografía infantil (ordenadores zombis), o para obtener dinero (*ransomware*).

D) *Virus informáticos:* son programas con unas características muy peculiares que se introducen en los ordenadores de formas muy diversas: a través del correo electrónico, Internet (…) Se reproducen infectando otros ficheros o programas o bien, al ejecutarse, realizan acciones molestas y/o dañinas para el usuario, ralentizando o apagando el sistema. El término virus informático se debe a su enorme parecido con los virus biológicos, se introducen en los ordenadores e infectan ficheros insertando en ellos su "código". Cuando el programa infectado se ejecuta, el código entra en funcionamiento y el virus sigue extendiéndose. Es la amenaza más conocida por su volumen de riesgo. (SITEMAP de tecnología)

E) *Hacker, hackeo:* hace referencia a las actividades que buscan comprometer los dispositivos digitales, como ordenadores, teléfonos inteligentes, tabletas e incluso redes enteras. Y aunque el hackeo puede no tener siempre fines maliciosos, actualmente la mayoría de las referencias tanto al hackeo como a los hackers, se caracterizan como actividad ilegal por parte de los ciberdelincuentes, motivados por la obtención de beneficio económico, por protesta, recopilación de información (espionaje), e incluso sólo por la "diversión" del desafío (Malware, s.f.).

F) *Aplicaciones web:* Pérez (2012), las define como soluciones informáticas que los usuarios utilizan accediendo a un servidor web a través de Internet o su red interna (intranet). Como interfaz con la aplicación se utiliza un navegador de Internet. Dicho de otra forma, es un tipo de software diseñado para funcionar sobre un servidor web y ser visualizado mediante un navegador (p.10)

G) *Comunidades virtuales*: entendidas como agregaciones de individuos que encuentran en el ciberespacio la posibilidad de interactuar, movidos por inclinaciones en común. Uno de los principales investigadores del fenómeno, Howard Rheingold, las ha definido como «agrupaciones sociales que emergen de la Red cuando suficientes personas sostienen discusiones públicas de gran duración con suficiente sentimiento humano como para formar webs de relaciones personales en el ciberespacio» (citado en Ciro, 2009)

2.6 Análisis del término derecho informático

En esta investigación se hace necesario realizar un estudio del término "derecho informático" en virtud de que el objetivo general propuesto es analizar la especificidad de la configuración típica de los elementos normativos de los tipos penales informáticos de estafa

informática, suplantación de identidad y difusión de información falsa, de ahí que el termino informático resulta primordial.

Con los cambios acelerados y constantes en el campo de la informática y las TIC, se hace necesaria la implementación de modificaciones o adaptaciones en lo relacionado al derecho y la aplicabilidad de justicia en ámbitos tan específicos como los delitos informáticos. Téllez (1991) define derecho informático como "una rama de las ciencias jurídicas que contempla a la informática como instrumento y como objeto de estudio" (p. 13).

En la misma línea de pensamiento, Verdugo (2011) escribe que:

> (…) el Derecho Informático es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas que brotan de la actividad informática. Se deduce de este concepto que la Informática en general desde este punto de vista, es un objeto regulado por el Derecho.
>
> La informática, como uno de los fenómenos más significativos de los últimos tiempos (…) deja sentir su incontenible influjo en prácticamente todas las áreas del conocimiento humano dentro de las cuales el derecho no puede ser la excepción, dando lugar a una nueva interdisciplina conocida como el derecho informático (p. 22).

Por su parte, Rodríguez (s.f.), reafirma la importancia del derecho informático al aseverar que:

> (…) el derecho informático debe elaborar el nuevo concepto de daño tecnológico o daño informático, delitos tecnológicos, delitos informáticos (…), se trata de aspectos jurídicos normativos orientados a la protección de intereses difusos, al afianzamiento pleno de la esfera de libertad de las personas (p. 27).

2.7 Derecho penal y teoría del delito

Como tema importante de esta teoría del delito, se encuentran la tipicidad, la antijuridicidad y la culpabilidad, para poder determinar la existencia o no de un delito y su respectivo autor. A partir de estos tres elementos, la teoría del delito instituye su base para establecer o dar fundamento a las teorías del caso en particular, cuando los operadores del derecho se enfrentan a determinados casos penales. Para esta investigación, se conceptualizarán la tipicidad y la antijuricidad. González (2008) argumenta:

> (…) la revisión de los elementos que conforman una conducta delictiva, se sustenta en el acaecimiento de una conducta o acción con relevancia para el derecho penal. Esto implica que el estudio de los tres elementos, tipicidad, antijuricidad y culpabilidad, no puede llevarse a cabo sobre una base abstracta, sino más bien concreta y ello solo ocurre, cuando se ha suscitado efectivamente una acción, entendiendo por acción una conducta humana (p. 80).

Entonces, según el autor, los elementos base son importantes para determinar la existencia de una conducta delictiva. En el caso de la tipicidad, Rojas y Sánchez, (s.f) indican:

> El tipo penal está constituido por la descripción de una conducta en el supuesto de hecho de una norma penal. La tipicidad es la adecuación de un hecho cometido, a la descripción que de ese hecho se hace en la ley. El tipo penal denota una norma que le es antepuesta y prohíbe la conducta. No deben confundirse ambos conceptos: la acción ejecutada por el autor es la acción prohibida por la norma, cuando se subsume en un tipo penal (p. 81).

Así que la tipicidad está en analizar si la conducta realizada se adecúa a la ley penal; si esta se refleja, se estaría hablando de una conducta típica. De lo contrario, si la conducta no se subsume en la ley penal, se llama conducta atípica; en este caso, deja de ser relevante para el derecho penal.

Como indica Bacigalupo (1996) “la coincidencia del hecho cometido con la descripción abstracta del hecho que es presupuesto de la pena contenido en la ley” (p. 95); es decir, el hecho cometido descrito en la norma, que a la vez obtiene una sanción.

En el mismo sentido, la citada acción típica dispuesta en la ley penal que se constata con los hechos presentados es prohibida, como indica Roxin (1997), “la acción típica ha de ser antijurídica, o sea prohibida. Por regla general lo será ya con la tipicidad, puesto que el legislador sólo incorporará una acción a un tipo cuando la misma usualmente deba estar prohibida” (p. 195). Sobre esta llamada antijuridicidad, expone Jiménez (1958) “Provisionalmente, puede decirse que la antijuricidad es lo contrario al Derecho. Por tanto, el hecho no basta que encaje descriptivamente en el tipo que la ley ha previsto, sino que se necesita que sea antijurídico, contrario al Derecho” (p. 267).

En cuanto a la tipicidad de los delitos informáticos, en Derecho.org (citado en Soto, 2001), se indica que:

> Por tratarse de conductas que, en cuanto suponen de agresión contra el interés del titular de un determinado sistema; de que la información que en él se contiene no sea interceptada, resultan tanto más reprochables, y aún merecedoras de sanción penal (si como suele ser lo habitual), atentan contra sistemas o equipos informáticos particularmente relevantes, que por razón del contenido de la información que procesan o almacenan y por las funciones que tienen asignadas en el seno de las relaciones jurídicas, económicas y sociales afectan gravemente a un interés supraindividual o colectivo (p. 6).

En relación con el tema de la tipicidad de los delitos informáticos en Costa Rica, se puede decir que, los especialistas en derecho penal, tanto nacionales como internacionales, tienen muchos obstáculos, entre estos, cómo determinar cuál de las conductas ilícitas se puede adecuar al tipo

penal de una forma apropiada a la ley penal actual costarricense y cómo se puede sancionar adecuadamente, según la participación.

Asimismo, el derecho penal mínimo destaca, en su sentido específico, otras sanciones menos gravosas; sin embargo, el principal problema que pueden enfrentar los fiscales, defensores y jueces es determinar el sujeto activo de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), los cuales presentan problemas en la tipicidad y en el reproche que se haga a los individuos infractores de la ley. La problemática de estos delitos informáticos, como se verá más adelante, es poder identificar quién o quiénes son los autores inmediatos de delito.

Otro punto es la amplitud que pretende abarcar el tipo penal de estafa informática y, además, lo complejo de su terminología, aspectos que son relevantes para esta investigación y que posteriormente serán analizados.

En cuanto a la teoría del delito, se determina si el imputado debe o no perseguirse por el hecho que se le acusa, de igual forma se analiza el bien jurídico y si la acusación que realiza la fiscalía debe continuar. En este sentido, señala González (2008):

> La teoría del tipo complejo organiza los elementos del delito de la siguiente forma: Tipicidad: La divide en tipicidad objetiva, donde se encuentran los elementos normativos, descriptivos y subjetivos; y subjetiva, donde se encuentra los elementos alternativos de dolo y culpa, ambos compuestos de elementos cognitivos y alternativos de dolo y culpa. En el caso del dolo, la acción debe ser realizada con conocimiento del hecho que se realiza y voluntad de llevarlo a cabo (nótese que no incluye el conocimiento de la ilicitud del hecho que se mantiene ubicado en la culpabilidad), y en el caso de la culpa, el aspecto cognitivo

> es la previsibilidad del resultado y el volitivo, el deseo y aceptación de los medios contrarios a derecho (p. 114).

Finalmente, con relación a la autoría y la participación, ambos son factores esenciales en la presente investigación, por lo que es fundamental conceptuar ambos conceptos. Señalan Rojas y Sánchez (s.f):

> El concepto de autor en el derecho penal no plantea ninguna duda, cuando una sola persona realiza el hecho punible. Se habla en este caso de autor directo, inmediato o unipersonal. No ocurre lo mismo cuando varias personas intervienen en la realización del hecho. En estos casos, se hace necesario identificar quién ha llevado a cabo el papel más importante y los que han mantenido una función secundaria; es decir, se trata de señalar al autor y a los partícipes (p. 355).

Al hablar del delito informático, el hecho de poder establecer una cantidad de autores y participantes es difícil, debido a que el medio empleado los hace permanecer anónimos en cierto sentido, de ahí lo complicado de poder imputar y clasificar, uno a uno, en caso de que sean varios los delincuentes. Como indica Lemaitre (2020), "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" (p. 119).

2.8 Análisis de tipos penales informáticos según el Código Penal costarricense

Son varios los delitos informáticos tipificados en Costa Rica desde el año 2001, previstos en el Código Penal. Aunque existen otros delitos informáticos tipificados en el Código Penal de Costa Rica, únicamente se hará referencia a los que atañen al presente estudio: fraude informático, artículo 217 bis, luego modificado a estafa informática en el año 2012); suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236). Esos artículos, específicamente los

dos primeros, fueron modificados por una serie de problemas que se observaron en la Asamblea Legislativa, por parte de Servicios Técnicos y otras instancias.

En relación con lo mencionado, Rivera (2001) realiza cuatro aseveraciones importantes; a saber:

> 1.- Las descripciones son muy extensas. En los tres artículos planteados se consignan veinte verbos y, en consecuencia, se trata de veinte acciones incriminadas, mezcladas en artículos de mucha amplitud.
>
> 2.- Los nuevos artículos contienen una serie de elementos normativos, cuyo significado es necesario determinar para comprender cuáles son las conductas tipificadas y a partir de ello valorar diversos aspectos, como los dogmáticos o constitucionales.
>
> 3- Las definiciones de los elementos normativos presentes en los artículos presentan un rasgo común: que son muy complejas y técnicas. Esta circunstancia ocasiona problemas porque hace más difícil la interpretación y aplicación de los tipos.
>
> 4.- La redacción de los tipos penales no es diáfana, se lesiona la función esencial en ellos, de proveer seguridad jurídica a los administrados, en el tanto no permiten determinar con claridad cuáles son las conductas por las que puede serles impuesta una sanción. De esta manera, nos encontraríamos frente a una violación del principio de legalidad, con el posible roce constitucional que ello conlleva (p. 83).

Estas razones fueron dadas para modificar el artículo 217 bis (luego, modificado a estafa informática en el año 2012), suplantación de identidad (numeral 230), modificado en el año 2013, por lo que se dio la respectiva reforma y la modificación a varios artículos mediante la Ley N.º 9048. También, se creó la sección VIII en el Código Penal llamada “Delitos Informáticos y

Conexos", en el año 2012. Esta última tuvo una reforma mediante Ley N.º 9135 en el año 2013, que permitió añadir otros delitos informáticos.

Para efectos de esta investigación, se visualizan, específicamente, tres tipos penales: a) la estafa informática, b) la suplantación de identidad y c) la difusión de información falsa. Todos estos delitos tienen en común el lapso de ejecución, factor que dificulta mucho la labor investigativa y la determinación del sujeto activo, expresa Bonilla (2019):

> Debe tenerse en cuenta que, tanto los delitos cometidos por medios informáticos, o bien como objeto de la actividad delictiva, tienen en común las siguientes características: De rápida ejecución y alto alcance: Esta clase de delitos puede ser realizados de forma sumamente rápida (p. 223).

Este análisis es consecuente con las ideas ya expuestas por otros autores. Se concuerda con el hecho de que estos delitos se caracterizan por su difícil tratamiento y la persecución, ya que, como se ha dicho, se ejecutan de manera rápida y provocan consecuencias patrimoniales fatales para las víctimas. La propia tecnología impide que quede rastro tras su uso.

2.8.1 La estafa informática.

En el caso de Costa Rica, este delito de estafa informática se ha previsto en el numeral 217 bis del Código Penal, que establece:

> 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 debido a sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
>
> *(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° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal").* (Poder Judicial, 2017)

2.8.1.1 Concepto de estafa. En primera instancia, se requiere la conceptualización y análisis de los delitos en estudio. Al respecto, De la Mata (2007) establece que:

> La estafa se define por la utilización de un engaño bastante que, generador de un error en otro, favorece una disposición patrimonial de éste, en perjuicio propio o de un tercero. En este contexto, ha sido largamente debatido el tratamiento que ha de darse a aquellos supuestos en que lo que se consigue la disposición patrimonial. Y en el ámbito estrictamente informático, el tratamiento que ha de darse aquellos supuestos en que se produce una manipulación en sistemas digitales con la que se logra una transferencia patrimonial (pp. 66-67).

Resulta importante lo aportado por Lemaitre (2020), quien asevera que en la estafa informática “no se ocupa la colaboración del sujeto pasivo (la víctima), sino que solamente es necesario manipular los sistemas informáticos para conseguir el resultado patrimonial” (p. 115).

De esta forma, con la sola manipulación de los medios tecnológicos, el delincuente puede concretar el delito, sin mediar interacción con la víctima, incluso sin que esta se entere de la situación de la que fue objeto. Este caso se contrapone con la estafa original, en la que se utiliza el ardid o el engaño, atrayendo a la víctima para hacerla incurrir en error y donde se hace necesaria su participación.

Con respecto a esa diferenciación del tipo de estafa, escribe Faraldo (2007):

> Frente a la estafa común, además de por la ausencia de engaño y error, la estructura típica de la estafa informática se caracteriza por el hecho de que la disposición patrimonial se consigue valiéndose el autor "de alguna manipulación informática o artificio semejante (…) Por su parte, el acto de disposición patrimonial, en este caso la transferencia de activos patrimoniales, no es realizado por la víctima del engaño, como en la estafa común, pues aquí no suele haber contacto humano, sino por el propio autor, generalmente a través del sistema (p. 36).

Dentro de este tipo penal, como se ha evidenciado, es importante recalcar que la estafa tradicional y la estafa informática se diferencian, principalmente, en que en la segunda no es necesaria la participación de la víctima de forma activa, puesto que como indica Lemaitre, (2020): "Solamente es necesario manipular los sistemas informáticos para conseguir el resultado de beneficio patrimonial" (p. 115). Asimismo, este delito solo puede ser cometido mediante un sistema automatizado de información, el cual define Lemaitre (2020) como "un conjunto de elementos relacionados entre sí, que se encarga de procesar manualmente y/o automáticamente datos" (p. 116).

Este sistema automatizado, que prevé el supra citado artículo, se conforma por tres variables: el sujeto que utiliza el sistema, los datos tanto de entrada y salida como los almacenados y, por supuesto, el medio tecnológico utilizado: computadoras, dispositivos USB, entre otros.

Los componentes esenciales del tipo ***objetivo*** del delito de estafa informática se describen en los siguientes subapartados.

2.8.1.1.1 Bien jurídico tutelado. Castillo (2016), citado por Lemaitre (2020), señala que el bien jurídico a proteger es el patrimonial. Sin embargo, 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 perjuicio sobre el sujeto pasivo; entonces, es posible no afectar el patrimonio de un sujeto pasivo y, de igual manera, cometer el delito.

Por otra parte, tanto la estafa informática como la tradicional, lesionan bienes jurídicos de corte patrimonial y, para distinguir una de otra, el término que se utiliza es delincuencia informática. Dicho término es definido como: “crimen electrónico que tiene como fin destruir los ordenadores, medios electrónicos y redes de internet, además incluye delitos tradicionales como falsificación, fraude, robo, extorción, entre otros, que son delitos cometidos mediante computadoras y equipos tecnológicos” (Ugarte, Acosta, & Soto, 2015, párr. 19).

Es importante la conceptualización que realiza Bonilla (2019), sobre el bien jurídico tutelado:

> En cuanto a los bienes jurídicos tutelados en esta clase de delitos se consideran como tal, la “información”, entendiéndose esta de forma amplia, involucrando en ella, documentos, bases de datos, expedientes electrónicos, cuentas bancarias, información médica,

> información industrial, etc., la cual de violentarse, podrá influir de forma transcendental en la vida de un individuo o de la colectividad, y conforme con el impacto presentado, podrá transgredir sustancialmente el desarrollo económico de uno o varios países, pudiendo llegar en pocos minutos a la catástrofe internacional (p. 224).

Existen varias opiniones doctrinarias en cuanto a cuál o cuáles son los bienes jurídicos tutelados en el delito de estafa informática, donde prevalece lo patrimonial y lo monetario. Del mismo modo, la información o los datos personales son valorados como un bien jurídico tutelado, mismo caso de la integridad de los datos de un sistema.

Se deben considerar ambas posiciones, pues en definitiva se protegen el patrimonio y los datos personales en el sistema. Como referencia, señala Sánchez (2009), citado por Lemaitre (2020):

> Tras el estudio que se ha realizado, podemos concluir que el bien jurídico que protege el delito de estafa, siguiendo la opinión mayoritaria de la doctrina, es el patrimonio, entendido de forma amplia; a saber, como conjunto de derechos, bienes y relaciones jurídicas de que puede ser titular un sujeto; encuadrando, por tanto, este tipo delictivo, dentro de la categoría genérica, ya mencionada anteriormente, de delitos económicos de enriquecimiento, con la particularidad de tratarse de un tipo de delitos de apoderamiento (p. 121).

En este mismo sentido, se concluye con la idea de que el artículo 217 bis del Código Penal es confuso y requiere ser analizado, para realizar las modificaciones necesarias o bien, determinarse si es realmente necesario, ya que el artículo 216, del Código Penal, abarca la acción ilícita aun si se comete por medio de una computadora. Por otra parte, la doctrina no se ha puesto de acuerdo en cuanto a cuál es el bien jurídico tutelado, de hecho, las características indican que es el patrimonio.

2.8.1.1.2 Sujeto activo. En el delito de estafa informática, el sujeto activo es cualquier persona física que se presume tiene conocimiento en informática y tecnología; el sujeto pasivo puede ser cualquier persona física o jurídica. Quien es considerado como sujeto activo es, generalmente, el último eslabón de la cadena, el que retira el dinero, pero quien comete el delito, desde el engaño hasta la manipulación del sistema informático, se enmascara en la tecnología y es casi imposible de rastrear.

Esta situación provoca, además, que ante la imposibilidad de demostrar la participación dolosa del llamado "frentiador" este quede libre, pues, no hay elementos probatorios que lo relacionen con algún tipo de organización criminal o con el hecho de declarar que nunca existió intención de cometer ese delito, que fue engañado. En este sentido, hay que recordar que, en este tipo de criminalidad, quienes aparecen procesados no son los sujetos activos; es decir, quienes cometieron el ilícito detrás de las computadoras, sino las personas a las que se les ha depositado el dinero proveniente del ilícito.

Al ser un delito informático, el hecho de poder establecer una cantidad de autores y participantes es difícil, debido a que el medio empleado los hace permanecer anónimos en cierto sentido, de ahí lo complicado de poder imputar y clasificar, uno a uno, en caso de que sean varios los delincuentes. Como indica Lemaitre (2020), "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" (p. 119).

2.8.1.1.3. Verbos y acción típica. Con respecto a la acción penal propiamente, Lemaitre (2020) asevera que "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 en un sistema" (p. 120).

En este tipo penal, se establecen varias formas de cometer el delito: a partir del verbo "influir", desde la óptica de la informática, según lo previsto al inicio del artículo 217 bis del Código Penal que, según la definición de Lemaitre (2020) significa: "Producir un efecto sobre las operaciones de un conjunto de datos o del resultado final de esos datos" (p. 117).

Dentro de las formas previstas para la comisión de este delito se tienen, principalmente:

a) El uso de datos falsos o incompletos que, según La web del programador (2018), citado por Lemaitre (2020), son: "Hechos y cifras en bruto, tales como órdenes y pagos, los cuales se procesan para obtener información, por ejemplo, el saldo deudor y el monto disponible" (p. 118).

b) Uso indebido de datos: Según Castillo (2016), citado por Lemaitre (2020) "en este caso nos encontramos que, aunque los datos sean correctos o veraces, la persona que los utiliza no está autorizada o no es la titular de los datos para ser utilizados, en el sistema automatizado" (p. 118).

Se puede sintetizar además que, en el delito doloso de estafa informática, se distinguen, como acciones típicas:

a) El robo o falsificación de tarjetas de crédito o débito. Ya sea por clonación o sustracción de las tarjetas, los delincuentes realizan retiros o bien utilizan las tarjetas falsas para retiros o transacciones en comercios, si se considera que existe manipulación al sistema bancario.
b) Manipulación o intrusión en el procesamiento o resultado de datos de un sistema automatizado de información. Como es el caso de una intromisión en sistemas financieros para realizar movimientos bancarios, entre cuentas, generalmente se utilizan cuentas de terceros, que pueden o no saber el origen de los montos de dinero girados.

Aunque el engaño parece ser parte del delito, no constituye una estafa informática, pues para que esta acción exista debe haber uso de la tecnología para perpetrar el dolo, por lo que cuando los delincuentes se valen de ardides muy creíbles, como llamadas en las que se identifican como

personeros de alguna entidad bancaria, supuestas compran de bienes, o bien, supuestas actualizaciones de datos personales y con ello logran acceder a claves o números de cuentas, esta acción sería típica de la estafa común, pues la manipulación del sistema informático o base de datos es el ciberdelito.

Cuando se está ante una estafa informática, se presupone la existencia de un daño al *software*. De no existir ese daño, el fraude cometido se valora como una estafa tradicional, pues, aunque se utiliza una computadora, con la cual el sujeto activo consigue un perjuicio patrimonial al sujeto pasivo y, a la vez, un beneficio patrimonial para él mismo o para terceros, no hay daño al sistema informático. Se evidencia el delito de fraude y lo que se comete es una estafa pura y simple, ya tipificada en la ley penal. Esta situación evidencia un problema en la tipicidad del delito como tal.

2.8.1.1.3 Tipo subjetivo. En relación con este tipo de delito informático, el cual implica una acción dolosa, tal como lo señala Lemaitre (2020): "El tipo subjetivo implica, en este caso, una acción dolosa, donde el sujeto activo busca un beneficio, es su intención" (p. 122).

Sobre el tipo subjetivo, agrega González (2008) que:

> Cuando se señala el tipo subjetivo, se alude al origen interno de dicha conducta. Lo que interesa es establecer bajo qué circunstancia, la misma se ha generado. Si la misma ha sido realizada con una intencionalidad definida o si, por el contrario, la misma es el resultado de una actuación que falta al deber de cuidado que la sociedad moderna impone en cada una de las tareas que ejecutemos (p. 134).

Es importante agregar que, en este tipo penal, se prevén dos situaciones: una, la sola intención de procurar y, la otra, obtener el bien, es decir, como indica Castillo (2016), citado por Lemaitre (2020): "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" (p. 119). Es así como este delito es de peligro abstracto, es decir, no requiere de un resultado concreto para que se configure, la sola intención o manipulación de datos personales es sancionable como delito.

2.8.1.1.4 Aspectos de relevancia jurídico-penal. El artículo 217 bis del Código Penal es claro en especificar la pena por el delito de estafa informática con tres a seis años o bien, de cinco a diez; sin embargo, dentro del mismo artículo, existen aspectos fundamentales que deben ser analizados, pues podrían caer en una amplitud riesgosa, para su aplicabilidad o bien, ser confusos en su semántica.

Establece que el perjuicio puede darse en contra de persona física o jurídica, lo que indica que el sujeto pasivo puede ser cualquier individuo o incluso empresas y entidades públicas o privadas.

Dos términos vitales que deben ser esclarecidos en el artículo 217 bis son: datos e información. Aunque en ocasiones se utilizan como sinónimos, estos términos tienen, cada uno, su significación y utilidad en el ámbito informático. Bulmaro Noguera (s.f.) explica que: "Un **dato** no es otra cosa que una representación simbólica de alguna situación o conocimiento, sin ningún sentido semántico, describiendo situaciones y hechos **sin transmitir mensaje alguno**. Puede ser un número, una letra o un hecho" (párr. 3, el resaltado es del original).

Con respecto al término información, explica Noguera (s.f.) que:

> Es un conjunto de **datos**, los cuales son adecuadamente procesados, para que de esta manera, puedan proveer un mensaje que contribuya a la toma de decisión a la hora de resolver un problema, además de **incrementar el conocimiento**, en los usuarios que tienen acceso a dicha **<u>información</u>** (párr. 4, el resaltado es del original).

Como se evidencia, un dato es, por ejemplo, una serie de números que, sin un contexto no tiene significado, pero que también podría ser una cuenta bancaria y la información es el conjunto de esos números utilizados para representar bienes; en ese caso, dinero propiedad de un individuo. La información es, entonces, como explica Noguera (s.f.), más extensa y con mayor significación.

Aparece también el concepto de sistema automatizado de información. Fábregas (1991) señala que es un "conjunto de elementos humanos y electrónicos que se combinan para procesar datos que serán utilizados para la toma de decisiones" (p. 25). Estos datos pueden ser ingresados voluntariamente por las personas, por ejemplo, en una red social como Facebook, donde los usuarios incluyen datos personales que serán almacenados en bases de datos y serán manipulados por los responsables de la red social.

Alfons (2000) manifiesta que una base de datos es "un conjunto de datos no redundantes, almacenados en un soporte informático, organizado de forma independiente de su utilización y accesible simultáneamente por distintos usuarios y aplicaciones" (p. 14).

Lo mismo ocurre con las entidades bancarias, por ejemplo, donde la información debe ser protegida por el sistema, aunque muchas veces, pese a las advertencias, son los mismos tarjetahabientes quienes facilitan números de cuentas y claves de acceso y se convierten en víctimas de estafas.

El artículo 217 bis aduce un manejo de la tecnología que, pareciera, solo está en manos de personas que tienen conocimientos en el área de la informática, pues la comprensión del leguaje técnico de la informática se le debe dar especial atención: palabras como "hackear" o, como se indica, realizar una "operación informática o artificio tecnológico". Aquí se llega a otro concepto clave, operación, el cual se define como: "una instrucción para que sea concretada por una computadora" (Porto & Merino, 2009, párr. 10).

También, se menciona el término “artificio”, la RAE lo define como: “Del lat. *Artificium,* (…) 3. m. artefacto (objeto construido para un determinado fin)”. Este concepto aduce que, para considerarse delito, según el Código Penal, este debe estar involucrado un artefacto tecnológico.

En el caso de una persona que mediante engaños obtiene la clave de un tarjetahabiente, este utiliza una tarjeta de crédito o débito, que no es de su propiedad y extrae dinero o realiza compras, ¿se considera estafa informática si no se vulnera el sistema bancario, hay realmente una instrucción informática en ese delito? ¿Existe, además, un delito de suplantación si ese individuo se hace pasar por el dueño de la tarjeta para realizar transacciones? Sin duda alguna, este cuestionamiento es clave a la hora de tipificar el delito, pues, en algunos casos, se cataloga como estafa informática y, en ese caso, se regiría por el artículo correspondiente 217 bis.

Ahora bien, tener claro el tipo penal es imprescindible para el proceso judicial y es por ello que la normativa no debe dar lugar a ambigüedades o interpretaciones diversas. Debe ser tan clara que no exista duda alguna.

La pena que establece el artículo 217 bis se agrava si quien la comete es un individuo con acceso al sistema, si es de naturaleza pública de bancos o si hay relación laboral con la entidad vulnerada, situación que es también difícil de demostrar pues, como se ha explicado, el ciberespacio es el lugar prefecto para ocultarse. Se puede cometer el delito desde cualquier parte del mundo y hacer desaparecer la huella digital para no ser identificado.

Otro aspecto que no se contempla en el 217 bis es el hecho de que las estafas informáticas pueden ser realizadas fuera del ámbito nacional por lo que, la determinación del sujeto activo es aún más difícil, por no decir imposible.

La redacción del artículo en análisis requiere una revisión en la que se involucren expertos del área informática y del derecho para que, en trabajo conjunto, se cierren portillos de

interpretaciones y terminología poco clara, que permitan eliminar esa condición de amplitud que posee.

Ahora bien, un aspecto relevante es la cantidad de términos que forman parte del artículo 217 bis, llamado estafa informática, entre ellos: 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.

Estos términos tienden a ser confusos y complejos; palabras como procesamiento, sistema automatizado, programación, operación informática o artificio tecnológico son sumamente técnicos y de difícil comprensión. Hay que destacar que, en este artículo, queda un vacío cuando se lee lo siguiente: “o bien, por cualquier otra acción”, lo cual crea la sensación de que el legislador quiso abarcar mucho y, sin duda, es uno de los términos más oscuros en dicha norma ya que es muy amplio. Se evidencia, en el artículo mencionado, que el legislador deja una amplitud peligrosa al señalar cualquier otra acción, lo que genera incertidumbre en su aplicabilidad.

Hay que hacer notar que, en el estudio de este delito, se han encontrado algunas diferencias entre la estafa tradicional y la estafa informática. En esta última, no existe un engaño a la víctima de manera directa, sino que hay una manipulación del sistema con la idea de tener un beneficio de corte patrimonial.

2.8.2 Suplantación de identidad.

En la ley costarricense, este delito se encuentra previsto en el artículo 230 del Código Penal, que dicta:

> Artículo 230. Suplantación de identidad. Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. *(Así adicionado por el artículo 3° de la Ley N.º 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal") (Así reformado por el artículo 1° de la ley N.º 9135 del 24 de abril de 2013).* (Poder Judicial, 2017).

2.8.2.1 Concepto de suplantación de identidad. Se denomina de esa manera a cuando se sustituye o usurpa la identidad de otro individuo; por ejemplo, en una red social una persona se hace pasar por otra en un perfil falso. Sin embargo, no queda claro este tipo penal, pues se indica que debe mediar el uso de un medio informático en la comisión, pero no existe ninguna afectación a un software. De esta forma, si no existe una afectación, entonces no habría delito informático como tal; es decir, podría ser un delito cometido a la identidad de la persona, por el que podría ser procesado el sujeto activo, pero no como delito informático, pues no cumple con la característica de este tipo de infracción.

En definitiva, la identificación de una persona es un bien invaluable y, cuando un delincuente decide suplantar a su víctima para sacar provecho, se trata, inequívocamente, de fraude. Como tal, requiere una legalidad que aplique sanciones concretas y correctas.

De manera que se conceptualizarán los términos: identidad y suplantación de forma separada. Primero, se establece el término identidad:

> Del lat. tardío *identĭtas, -ātis,* y este der. del lat. *ídem* 'el mismo', 'lo mismo'. Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás. Conciencia que una persona o colectividad tiene de ser ella misma y distinta a las demás (Real Academia Española, RAE, 2020).

Como se observa, es un concepto claro de individualidad y pertenencia. Por otra parte, en el argot jurídico se establece como identidad: "Conjunto de los datos en virtud de los cuales se establece que una persona es verdaderamente la que se dice o la que se presume que es (nombre, apellido, nacionalidad, filiación, etc.)" (Rogers, 2020, parr 1).

La identidad es, a su vez, un derecho humano, previsto y tutelado por normas internacionales. La Declaración Universal de Derechos Humanos, Artículo N.º 6, le otorga protección al derecho a la identidad al establecer que: "Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica" (Comisión Presidencial coordinadora de la Política del Ejecutivo en materia, 2011, p. 18).

Esta misma idea, la cual postula que la ley debe dar reconocimiento y ser garante de que se otorgue esa personalidad, viene establecida desde 1966, en el Pacto Internacional de Derechos Civiles y Políticos, en cuyo artículo N.° 16 se dictaba que: "Todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica" (Organización de Naciones Unidas, 1996-2020).

A nivel nacional, el derecho de identidad se encuentra estipulado en el artículo 23 del Código de Niñez y Adolescencia, Capítulo II, derecho de la personalidad, al establecer que las personas menores de edad tienen derecho al nombre, a la nacionalidad y a un documento de identidad y el compromiso a prestar asistencia y protección cuando se prive ilegítimamente de algún atributo de su identidad.

Al respecto del término suplantación, la RAE, indica “suplantar”: “Del lat. *supplantāre* 'derribar', 'zancadillear'. 1.tr. Falsificar un escrito con palabras o cláusulas que alteren el sentido que antes tenía. 2. tr. Ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba” (RAE, 2014). En términos legales, se considera suplantación como: “Quitar a una persona de su sitio de manera fraudulenta, ocupando su cargo o posición, o asumiendo sus funciones” (RAE, 2020). Como se evidencia, existe una connotación de fraude o delito correlacionada con el término “suplantación”.

Ahora bien, sobre cómo se concibe la “suplantación de identidad” como tal, Hernández (2019) explica que:

> La suplantación no es más que el hecho que realiza una persona para tomar la representación de otro ser, sea este en la vida cotidiana, en el ámbito civil, comercial o penal, esta acción la realiza de mala fe y con dolo, buscando el tan solo hecho de tener un beneficio particular causando daño al titular de esa información ya sea a su imagen, su integridad y en algunos casos hasta de forma económica (p. 31).

Como sinónimo de este término, se utiliza, “usurpación” que, del mismo modo, conlleva una connotación delictiva. Arreola (2017) explica que:

> La usurpación de identidad es relatada como una conducta antijurídica, dolosa, que emana de un individuo que maniobra la información personal de otro individuo, sin su autorización, con el ánimo de cometer una variedad de delitos, manipulando diferentes caudales para obtener la información íntima de una persona a través de un engaño hacía la víctima y al mismo tiempo, estilando incomparables tipos de medios Convencionales y Tecnologías de la Información y Comunicación (TICs) [sic], para realizar la conducta originándole un daño patrimonial o moral (p. 8).

Del mismo modo, Márquez (s.f.), con una visión más específica de la usurpación como delito expone que:

> El delito de usurpación de identidad radica en la conducta antisocial de una persona que se apropia o se apodera de una identidad que no le pertenece, es decir, pone bajo su poder y despoja al titular del bien jurídico de su identidad. Puede producirse con o sin violencia, porque puede ser despojado de sus pertenencias de manera violenta contra su voluntad o bajo amenazas, y posteriormente darles mal uso. La persona usurpada no se da cuenta de que ha sido violentado su derecho de manera indebida enterándose a posteriori.
>
> Se afirma que la usurpación de identidad puede cometerse por cualquier forma porque puede producirse a través de diversos trámites administrativos, contratos mercantiles, operaciones fiscales o crediticias, documentos robados, extraviados o mediante venta ilegales aun cuando el uso más frecuente es a través de los medios electrónicos o telemáticos (pp. 341-342).

Los componentes esenciales del tipo ***objetivo*** del delito de suplantación de identidad se describen en los siguientes apartados.

2.8.2.1.1 Bien jurídico tutelado. En este delito, el bien jurídico es la identidad del sujeto pasivo físico o jurídico. La consideración de identidad como un bien único y específico de cada ser humano es explicada por Gómez (2017) al escribir que:

> la identidad en primer lugar está formada por la percepción más o menos estable que la persona tiene de sí misma y de las cualidades, los defectos y los recursos que le son particulares como alguien único y diferente de todos las demás (p. 29).

Desde el razonamiento como un bien tan personal, el uso de la identidad de otro individuo, con fines ilícitos, deriva directamente en una acción delictiva.

La suplantación de identidad, en la mayoría de los casos, pretende y logra el robo de datos o bien, el uso de información personal, sin autorización; al respecto se afirma que:

> Actualmente, las personas son expuestas con sus datos personales, por acciones inocentes, como llenar encuestas de satisfacción, supuestas rifas, las inscripciones en eventos, es decir, formas de apropiarse de datos personales sin consentimiento informado, o bien, con consentimiento informado, pero con letra muy menuda; asimismo, existen otro tipo de acciones, como compartir fotos, etiquetar personas en redes sociales sin consentimiento transmitiendo datos personales, que desembocan en problemas como espionaje informático, uso fraudulento o usurpación de identidad (Rivera, 2019, párr. 13).

Como explican Guerrero y Salazar (2014), el objetivo de la norma en el delito de suplantación, es proteger la identidad, que como ya se ha analizado, es un derecho innato de cada persona.

> Lo que se pretende proteger sancionando la suplantación es el derecho a la identidad propia y reconocida de cada persona y a la protección de los derechos de autor de quien posea una página de internet, situaciones que no tienen por qué depender del medio a través del cual se violenten (p. 255).

Este tipo de delito no afecta un solo bien jurídico, sino una pluralidad de ellos, como indican Magliona y López (citados en Acurio Del Pino, 2010), al aseverar que existe un carácter de pluriofensivos, es decir, “que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo” (p. 10).

Con respecto al bien tutelado en la suplantación, también se da esa variedad en la afectación. Escribe Romero (2010), que el tipo penal debe proteger:

> (…) una serie de intereses jurídicos en el contexto de la suplantación de identidad, tales como los intereses patrimoniales de la persona cuya identidad se suplanta, la privacidad de las personas a quienes sus datos personales les han sido sustraídos o apropiados e inclusive podríamos extender su tutela al ámbito de interés colectivos para garantizar la veracidad en las relaciones sociales a partir de Internet, en particular de las que se emprenden a través de las Redes Sociales (pp. 856-857).

Ahora bien, en el expediente legislativo N.º 18546 de la Comisión Permanente Especial de Derechos Humanos, se proponen cambios en materia de suplantación de identidad.

> Sobre el artículo 230. (…) La suplantación de identidad también puede afectar directamente el patrimonio de un individuo, cuando dicha conducta se da en sitios que permiten la compra y venta de servicios, y el actor realiza una compra a nombre del sujeto pasivo, utilizando o no, datos de sus tarjetas de crédito o débito. Es por esto, que se agrega un agravante en los casos que el actor consiga afectar el patrimonio del sujeto pasivo u obtenga un beneficio patrimonial con la acción delictiva como lo que se denomina coloquialmente como “sicariato digital” (Asamblea Legislativa, 2012, p. 12).

Barrantes (2020), explica que, con el advenimiento de las TIC, deben protegerse los datos personales para evitar la suplantación.

> El uso de las Tecnologías de la Información y de la Comunicación (TIC) ha permitido que en muchas ocasiones los datos personales sean utilizados para fines distintos a los que originalmente fueron recabados, es decir, son transmitidos a otras instancias distintas de las que la persona dueña de los datos confió información, violentando su privacidad, por lo que, bajo el concepto de protección de datos personales, el titular tiene el derecho y la

> libertad de elegir qué desea comunicar, cuándo y a quién, manteniendo el control sobre su información personal.
>
> Por lo anterior, nace la Ley N.º 8968 Protección de la Persona frente al Tratamiento de sus Datos Personales y su Reglamento, con el fin de garantizar a cualquier persona, que los derechos fundamentales deben ser respetados (Barrantes, párr.1-2).

2.8.2.1.2 Sujeto activo. El delito de suplantación de identidad, desde su concepción como ciberdelito, presume un sujeto activo que, mediante el uso de la tecnología, se hace pasar por otro individuo o incluso, por empresas o corporaciones. Márquez (s.f.) establece, claramente, las categorías de sujeto activo y pasivo al explicar que:

> El sujeto activo del delito es la persona física que interviene en la comisión de un hecho ya sea como autor o como partícipe, no tiene ninguna calidad específica, es decir, la propuesta no exige que la persona tenga una característica especial (como ejemplo servidor público), por lo tanto, lo puede cometer cualquier persona (p. 345).

Este sujeto activo recibe el nombre de *phisher*, el cual, mediante el uso de medios tecnológicos, incurre en el delito:

> Haciéndose pasar por alguna empresa o institución de confianza, y utilizando la tecnología de la información y las comunicaciones, trata de embaucar al atacado para que le proporcione información confidencial, que posteriormente es utilizada para la realización de algún tipo de fraude (INTECO, 2007, p. 38).

Al respecto, Temperini (2012), citado en Montaperto (2018), explica que:

> En lo referido a los sujetos activos de la suplantación de identidad, son personas físicas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, que tienen habilidades para el manejo de los sistemas informáticos y generalmente

> por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de ilícito (p. 26).

2.8.2.1.3 Sujeto pasivo. En primer lugar, explica Temperini (2012), citado en Montaperto (2018), que la víctima puede ser cualquiera sin formación técnica en informática. En segundo lugar, ubica a las entidades comerciales, financieras y crediticias que realizan trámites sin una adecuada identificación del usuario o que tiene controles débiles y vulnerables.

Por último, ubica Temperini (2012) al Estado como sujeto pasivo, quien, al actuar negligentemente, se vuelve en parte responsable, porque posibilita la comisión del ilícito, carece de normativa, no realiza campañas de concientización ni controles dirigidas al ciudadano y la protección de sus datos. Temperini (2012) termina su argumento señalando que existe dificultad para denunciar esos delitos.

El ya mencionado expediente N.º 18546 establece, también, modificaciones en materia penal, al indicar que:

> Se incluye como sujeto pasivo de la conducta penal a personas jurídicas y a las marcas comerciales, que también pueden ser víctimas en este tipo de delitos. Esta norma también aclara que este tipo penal es únicamente de acción privada, y no de acción pública. Se elimina el uso del concepto de “identidades falsas” o “inexistentes” ya que la conducta que buscaba tipificar en la anterior ley, era el de Grooming, la cual se está incluyendo en esta reforma y ha sido nombrada corrupción por vías electrónicas (Asamblea Legislativa, 2012, p. 8).

2.8.2.1.4 Verbo o acción típica. En un delito de suplantación de identidad, la acción típica es, evidentemente, la usurpación con fines ilícitos. Indica Arturo R, (2012) citado por Lemaitre (2020),

> Esta acción es cuando una persona se hace pasar por otra; en este caso, puede hacerse pasar por una persona física (persona) o jurídica (empresa) o de una marca comercial (nombre, término, signo, símbolo, díselo o una combinación de éstos que se le asigna a un producto, servicio o empresa con el fin de identificarlo y distinguirlo de los demás productos, servicios o empresas que existen en el mercado" (pp .140-141).

Sobre el campo de acción en este tipo delictivo, Hernández (2017) establece tres escenarios en los que se debe ubicar la suplantación de identidad: desde su ubicación física, en medios informáticos y por medio de telecomunicaciones. Cuando se utilizan medios tangibles (papel, plástico entre otros), para alterar o cambiar información de documentos o credenciales, por ejemplo, al sustraer una cédula de identidad y utilizarla como propia, se está ante una ubicación física.

En cuanto a los medios informáticos, Hernández (2017) asevera que este supone el uso de sistemas informáticos, utilizando distintos tipos de software, por ejemplo, los virus, para apropiarse de la información mediante correos electrónicos falsos. Por último, en lo referente a telecomunicaciones, explica el autor, se da por medio del teléfono o del internet. El delincuente finge ser otra persona y utiliza la información en su provecho.

Las empresas informáticas, preocupadas por el auge de este tipo delictivo, crean campañas de divulgación para que los usuarios puedan entender las acciones típicas de la suplantación de identidad y evitar caer en sus trampas. Un ejemplo de esas iniciativas es la empresa ACENS Technologies (s.f.) que explica que:

> El funcionamiento de este tipo de ataques para conseguir información relevante del usuario es muy sencillo. Lo primero que hace el atacante es crearse una apariencia de un ente de confianza.
>
> El siguiente paso sería realizar el envío de los mensajes por algún medio de propagación, mensajes que irán destinados a miles de usuarios. Entre estos usuarios, habrá un cierto porcentaje que se fiarán del mensaje y seguirán las instrucciones que indique el mensaje. Hecho esto, el usuario habrá proporcionado información de gran valor al atacante. Las consecuencias de esto principalmente son: • Robo de dinero de la cuenta bancaria. • Uso indebido de las tarjetas de crédito. • Envío de publicidad en su nombre. • Suplantación de identidad (p. 2).

2.8.2.1.5 Aspectos de relevancia jurídico penal. En el caso específico de Costa Rica, el delito de suplantación no es novedad, pues existen antecedentes y casos reconocidos. Al respecto se señala que:

> La suplantación de identidad es el tercer delito informático más denunciado en nuestro país, fue incorporado en nuestro Código Penal en el Artículo 230 desde el año 2012 y fue reformado en el año 2013 donde se extendió la protección a las personas jurídicas y a las marcas comerciales (Medrano, 2016, párr. 1).

El artículo 230, del Código Penal, establece prisión de uno a tres años por suplantar la identidad de otro, ya sea un ente físico, jurídico o incluso una marca comercial. Asimismo, delimita su rango de acción a redes sociales, sitios de internet o medios tecnológicos.

Se encuentra, entonces, una disyuntiva. Si un individuo roba la tarjeta de otra persona y compra, haciéndose pasar por el dueño del plástico, ¿no está acaso suplantando la identidad de la víctima y utilizando, para ello, un medio electrónico que en ese caso sería la tarjeta misma?, ¿se

considera suplantación o estafa? Por último, ¿tiene responsabilidad el dueño del negocio por no corroborar la identidad del tarjetahabiente?

El artículo 230 parece quedarse corto en su planteamiento. Se hace mención de las redes sociales, en el caso de un perfil falso, creado por un tercero con intenciones diversas, ya sea mortificar, dañar la integridad, el honor, el buen nombre, o bien, para injuriar o calumniar. Al parecer, hay inmersos más delitos que una simple suplantación de identidad; sin embargo, le hacen falta verbos que tipifiquen la acción específica.

En el caso de redes sociales, muchas veces la víctima no presenta la denuncia, se conforma con hacer notar a sus contactos que existe el perfil falso y reportarlo a su proveedor, por ejemplo, Facebook o Instagram. Estas, generalmente, proceden a cerrar la cuenta falsa sin que medie un proceso, para identificar al sujeto activo, en las entidades judiciales.

Del mismo modo que otros delitos informáticos, se presenta el problema de que la víctima no realiza denuncias formales, ya sea porque desconoce al infractor, o bien porque considera imposible que se descubra quién o quiénes realizaron el dolo y se conforman con que se borre el perfil, sin darle la importancia al hecho de la suplantación como tal.

Con el arraigo de las redes sociales y los sistemas de intercomunicación masiva, la suplantación de identidad se ha convertido en un mal constante y, tal como indica Hernández (2017):

> Personas con amplio conocimiento en sistemas informáticos, mediante el uso de programas maliciosos o virus, acceden de forma no autorizada a distintos sistemas informáticos, con lo que han logrado acceder a información sensible catalogada como confidencial, esta información suelen utilizarla de maliciosamente, perturbando de esta forma la integridad e identidad de las personas afectadas, en algunos casos han provocado ataques a la intimidad,

> dañado de esta manera el derecho al buen nombre que tiene cada ser humano, vulnerando su moral y en ocasiones de forma económica (p. 18).

Del mismo modo, Villacampa (s.f., citado por Faraldo, 2010) concuerda con que el uso de la tecnología ha favorecido la comisión de delitos de suplantación:

> La comisión de defraudaciones basadas en la suplantación de identidad se ha visto favorecida por la introducción de las nuevas tecnologías en las transacciones comerciales, en particular por la utilización de nuevos medios de pago en el comercio tradicional y por la generalización del comercio electrónico, en el que las tarjetas de crédito son el método de pago preferido (p. 88).

Para algunos autores, existe una divagación o un sinsentido de la tipificación de este delito como crimen informático, ya que, al fundamentarse en la suplantación de la identidad de una persona, se encontraría incluido en lo concerniente a la protección del derecho a la identidad, siempre que no se tenga como fin lesionar un *software* o medio informático.

Sobre esta divagación del concepto, se considera relevante la aseveración de Guerrero (2014), porque si en realidad no existe afectación a un *software*, no se debería estar tipificado como delito informático, lo que resulta importante desde el momento de presentar una denuncia, hasta el proceso de aplicación de la ley por los actores del derecho. El autor afirma que:

> No encontramos su justificación para constituirse como delito informático. Pareciera ser que la conexión que se pretende establecer radica en que la suplantación de identidad se realice en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información o que se suplanten sitios legítimos de la red de Internet. Pero, ¿eso qué relación tiene con intromisión en el software de un medio informático? Lo que se pretende proteger sancionando la suplantación es el derecho a la identidad propia y reconocida de cada

> persona y a la protección de los derechos de autor de quien posea una página de internet, situaciones que no tienen por qué depender del medio a través del cual se violenten (p. 255).

Como se ha dicho, se encuentra otro punto que requiere de un análisis más detallado; sin embargo, queda duda del delito informático, si con el hecho de tipificar una acción que no tiene ninguna afectación al software; la rapidez con que evolucionan este tipo de delitos ha tomado por sorpresa al mundo entero, no cabe duda de que existe preocupación internacional y en Costa Rica. Esto sin ahondar en el hecho de que la legislación internacional tiene gran influencia en cuanto a la dinámica de creación de tipos penales.

2.8.3 Difusión de información falsa

En la legislación nacional, este delito se encuentra previsto en el Código Penal, numeral 236. Difusión de información falsa:

> Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.
>
> *(Así adicionado por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal").* (Poder Judicial, 2017).

2.8.3.1 Concepto de difusión de información falsa. Se entiende por información falsa, aquella que no es verdadera en todo o en parte, con el objetivo de causar algún daño al sujeto pasivo. Otro término que se utiliza es el de *fake news* o, en su traducción al castellano, noticias falsas “es el concepto usado para identificar la divulgación de informaciones inexactas,

tendenciosas o simplemente falsas" (Wardle, 2019, párr. 1) que suelen circular por Internet o en las redes sociales.

Las *fake news* se caracterizan, además, porque son creadas con intención de engañar, lo que las distingue de la información errónea que se puede llegar a difundir. Como explica Wardle (2017), "poseen una intención premeditada, es decir que fue planeada o fabricada para engañar. Se puede diferenciar de lo que sería información errónea, la cual no implica difundir algo falso voluntariamente" (párr. 1).

La evolución de Internet y, principalmente, de las redes sociales, permite un tránsito acelerado de información y desinformación; se evidencia un cambio notorio en la manera en que el público se informa. Amorós (2018) explica que hay dos cambios importantes:

> Primero, las noticias ya no vienen con garantías, ya que tanto un hecho real y una noticia falsa, pueden viralizarse debido a la estructura de la misma red y su sistema económico de pago por clics. Segundo, las noticias llegan y se difunden dentro de burbujas de opinión, es decir, en nuestro propio círculo cerrado de quienes piensan como nosotros. Es así como, las noticias falsas se reafirman y se comparten de forma rentable para quien las crea (pp. 145- 146).

La facilidad con que las noticias falsas se propagan es preocupante y existen muchas formas para crearlas. Cortés e Isaza (2017) afirman que:

> Se trata de contenidos deliberadamente falsos que se publican en sitios web cuya apariencia intenta ser formal y auténtica. A veces el diseño del sitio y su URL suplantan un portal de noticias reconocido. El propósito claro es engañar al usuario. Generalmente estos contenidos se mueven en redes sociales a través de las cuentas propias de esos portales, ya sea de manera orgánica –mediante likes, retweets y compartidos de los usuarios– o con

> acciones promocionadas, es decir, pagando para que estos contenidos sean publicitados por las plataformas (p. 5).

En la misma línea de ideas, Amorós (2018) explica el panorama desde el punto de vista de la tecnología como herramienta de difusión y cómo ha cambiado el paradigma informativo:

> (…) antes, la información o las noticias llegaban a nosotros a través de los medios masivos tradicionales, los cuales se los tenía como emisor confiable, pero con las nuevas tecnologías móviles, la información viene suelta, las fuentes perdieron importancia, consumimos contenidos o nos gustan titulares que van con nuestra forma de pensar y simplemente los compartimos (p. 147).

La Revista Science, hace hincapié en la rapidez, alcance y amplitud de las noticias falsas y explica que es necesario el análisis de cómo se difunden, con qué intención y su influencia en los juicios de valor:

> Las nuevas tecnologías sociales, que facilitan el intercambio rápido de información y las cascadas de información a gran escala, pueden permitir la difusión de información errónea (es decir, información inexacta o engañosa). Pero, aunque cada vez más nuestro acceso a la información y las noticias está guiado por estas nuevas tecnologías, sabemos poco sobre su contribución a la propagación de la falsedad en línea (Soroush, Deb, & Sinan, 2018, párr. 2, traducción propia).

Wardle (2019) asevera que difundir información falsa es un proceso de desinformación con un claro interés en dañar y sacar provecho:

> La desinformación es contenido que es intencionalmente falso y diseñado para causar daño. Está motivado por tres distintos factores: ganar dinero; tener influencia política, ya sea extranjero o nacional; o causar problemas por ello (p. 8, traducción propia).

La autora agrega que esta difusión obedece, en muchos casos, al desconocimiento del emisor de que es falso lo que lee o bien, que concuerda con las ideas expuestas y se identifica, por lo que difunde los hechos sin corroborar, lo que facilita el trasiego de noticias o informaciones erróneas en todo o en parte:

> La desinformación también describe falso contenido, pero la persona que comparte no se da cuenta de que es falso o engañoso. A menudo una pieza de desinformación es detectada por alguien que no se da cuenta de que es falso, y lo comparte con sus redes, creyendo que están ayudando.
>
> El intercambio de información errónea está impulsado por factores socio-psicológicos. En línea, la gente realiza su identidad. Quieren sentirse conectados con su "tribu", si eso significa miembros del mismo partido político, padres que no vacunan a sus hijos, activistas que están preocupados por el cambio climático, o aquellos que pertenecen a una determinada religión, raza o grupo étnico (Wardle, 2019, p. 8, traducción propia).

Otro término que se considera importante es el llamado “bulo”. La RAE lo define como “Noticia falsa propalada con algún fin” (RAE, 2020). Este fenómeno se acrecienta con la propagación de imágenes, memes, videos, audios, cuyo contenido ha sido modificado o creado falsamente para lograr un objetivo concreto, como lo puede ser denigrar la integridad de una persona o incluso, un grupo social o una empresa.

En un contexto mundial, donde el ser humano parece tener cada vez mayor dificultad para distinguir entre verdad y ficción, surge el término “posverdad”, cuyo nacimiento se adjudica a la campaña electoral de Donald Trump y al Brexit, en Reino Unido. El término “posverdad” fue incluso catalogado por Oxford como la palabra del año en el 2016, y tiene como característica el hecho no de mentir, sino de ignorar la verdad; apela al sentimiento de las personas y las hace

reafirmar sus opiniones. Según escribe Gascón (2018): "El *Oxford English Dictionary* la define como una situación en que los hechos objetivos son menos determinantes que la apelación a la emoción o las creencias personales en el modelaje de la opinión pública" (párr. 1).

En el diccionario de la RAE se considera la posverdad como "Distorsión deliberada de una realidad, que manipula creencias y emociones con el fin de influir en la opinión pública y en actitudes sociales" (RAE, 2020).

Los componentes esenciales del tipo ***objetivo*** del delito de difusión de información falsa se definen en los siguientes apartados.

2.8.3.1.1 Bien jurídico tutelado. En el delito de difusión de información falsa, el bien jurídico es muy amplio según la situación específica. El autor Luis De Las Heras (2020) establece que pueden darse siete diferentes tipos penales y, en cada caso, se modifica el bien tutelado:

> (…) las noticias falsas son de tan variado contenido que, dependiendo de a qué se refieran y con qué intención sean difundidas, pueden llegar a integrar muy diferentes tipos penales" y referencia: 1) el delito de odio; 2) descubrimiento y revelación de secretos; 3) delito contra la integridad moral; 4) desórdenes públicos; 5) injurias y calumnias; 6) delitos contra la salud pública, estafas, intrusismo; 7) delitos contra el mercado y los consumidores (párr. 18).

Este autor, ubicado en la realidad española, ofrece una visualización sobre los tipos de bienes que se ven amenazados con la difusión de mentiras o falsedades: desde el honor, la intimidad, la propia imagen, hasta la información sensible de carácter económico y financiero, tanto de individuos como de grupos:

> Los ejemplos son numerosos y evidentes: 1) la mentira que es calumnia y, por tanto, hiere al derecho al honor (art. 205 CP); 2) la que es medio para producir error en otro

> induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno (art. 248 CP); 3) la difusión de noticias o rumores total o parcialmente falsos sobre personas o empresas con la finalidad de alterar o preservar el precio de cotización de un valor o instrumento financiero (art. 284.1. 2º CP) (De Las Heras, 2020, párr. 14).

De Las Heras (2020) agrega que, en el contexto de la pandemia de 2020, el patrimonio es, sin lugar a duda, otro bien que se ve en riesgo por la difusión de informaciones falsas:

> (…) unido a la actual situación de crisis sanitaria en la que se encuentra sumida nuestro país, constituyen el caldo de cultivo propicio para que algunas personas, aprovechando el desconcierto existente, traten de atacar determinados bienes jurídicos, entre ellos especialmente el patrimonio y singularmente el de aquellas personas que se encuentran en una mayor situación de vulnerabilidad (párr. 17).

Si bien es cierto lo expresado responde a la realidad de España, las coincidencias son evidentes en la realidad de muchas otras sociedades, incluida la costarricense.

La difusión de información falsa, o las llamadas *fake news*, se convierte en el insumo perfecto para la comisión de varias figuras delictivas *per se*, algunas de las cuales, según González (2020), por ejemplo, si se da la difusión de información de carácter personal o familiar se incurre en un delito de descubrimiento y revelación de datos personales, también delitos contra el honor, calumnias, injurias, al difundirse falsedades. Además, señala el autor, se podría cometer un delito de estafa, si existe beneficio monetario o incluso propiciar desorden y desestabilización social, si el bulo fomenta o incita al odio, violencia o discriminación contra un grupo o persona en específico, y se puede, incluso, derivar un delito de odio.

2.8.3.1.2 Sujeto activo. La acción de difundir información falsa presenta el inconveniente de que los sujetos activos borran su rastro y se esconden en el ciberespacio. La difusión de información falsa que, como se analizó, también llamada "fake news", posverdad y desinformación, tiene el inconveniente de que los sujetos activos no son fácilmente identificables, pues la tecnología facilita la comisión del delito tras una máscara, en muchos casos, infranqueable. Al respecto, se afirma que:

> El sujeto activo de esta clase de infracciones puede ser totalmente anónimo y usar este anonimato como forma de evadir su responsabilidad, ya que este no necesariamente puede usar su propio sistema informático, sino que se puede valer de un tercero, como por ejemplo en el caso del envió de correo no deseado o SPAM, en el cual se puede usar una máquina zombi, es decir una computadora que está bajo el control del SPAMER y que le permite usarla como una estación de trabajo de su propia red de máquinas zombis, las cuales pertenecen a usuarios desaprensivos que no tienen al día sus medidas de seguridad y que son fácil presa de los hackers y crackers para cometer este tipo de infracciones. También existen programas de enmascaramiento o que no permiten ver la verdadera dirección ya sea de correo electrónico o del número IP (Acurio Del Pino, 2010, p. 59).

El fenómeno del Internet y, especialmente, el de las redes sociales consideradas como las más comunes, Facebook y Twitter, han propiciado el incremento de delitos de difusión de información, con el agravante de ser fácilmente trasmitidos; sin embargo, en muchos casos, es casi imposible de rastrear la fuente. La tecnología permite utilizar los *bots* para la interacción con usuarios, lo que obstaculiza la identificación del sujeto activo.

El periódico *La Voz de Galicia* (2014) realiza una explicación de los llamados *bots* y cómo se utilizan. El medio informativo español señala que:

> La palabra bot viene de Robot y sirve para denominar en el argot tecnológico a las cuentas que simulan ser personas en una red social y son creadas con un fin determinado, bastante distinto al normal o habitual de un usuario que simplemente busca interactuar o convivir con otros. Los bots son generalmente llevados por un programa informático que realiza diversas funciones e imita el comportamiento de un humano, siempre de forma automática. Algunos de ellos cumplen funciones que vienen determinadas por un programador: publicar tuits con enlaces a una página web, retuitear de forma automática a alguien que mencione alguna palabra o hashtag... Los bots también son conocidos como usuarios fantasmas, cuyo único fin es el de inflar una cuenta y crear una falsa comunidad de admiradores (párr. 1).

Si bien es cierto, en algunos casos los *bots* se utilizan con fines publicitarios, para aumentar los seguidores de determinado personaje o hacer parecer que los tiene (lo que también constituye un engaño), la principal atenuante para el presente trabajo es el hecho de su uso para difundir falsedades. Al respecto, el ciberactivista mexicano Alberto Escorcia (2018) expone que esos *bots* van en aumento y, para quienes los utilizan, no importa si la información es falsa y que en diez años será más difícil distinguir entre realidad y mentira. El activista señala, además, que los responsables directos deberían ser las compañías como Google o Facebook que, aun detectando la existencia de esos perfiles o cuentas falsas, no las bloquean (Citado por Siu, 2018).

Para la delimitación o el establecimiento del sujeto activo más allá de los *bots,* se requiere analizar otros factores como quién etiqueta o a quién beneficia la difusión de información errónea, pues detrás de la automatización está el comportamiento humano.

> El comportamiento humano contribuye más a la difusión diferencial de la falsedad y la verdad que los robots automatizados. Esto implica que las políticas de contención de

> información errónea también deben enfatizar las intervenciones conductuales, como el etiquetado y los incentivos para disuadir la propagación de información errónea, en lugar de centrarse exclusivamente en restringir los bots (Soroush, Deb, & Sinan, 2018, párr. 21).

2.8.3.1.3 Verbo o acción típica. La acción típica de este tipo de delitos es precisamente difundir información que carece de verdad o bien que ha sido modificada con propósitos particulares.

Al respecto, se puede determinar que se comete el delito de difusión de información falsa cuando un sujeto infractor utiliza los medios tecnológicos como la electrónica, la informática o las telecomunicaciones para difundir noticias o hechos falsos con diferentes fines, principalmente, asustar, atemorizar, aterrorizar o menoscabar la identidad, honorabilidad de una persona física, jurídica o una marca, inclusive un país, creando descontrol social.

> La calidad de la información que maneja la opinión pública repercutirá en la capacidad de la misma de formar un pensamiento crítico y libre. Las *fake news* se oponen a este principio, al primar los contenidos sensacionalistas sobre las noticias contrastadas y racionales. Una democracia sólida no se puede explicar sin una opinión pública bien informada, que fomente un debate rico y que dé lugar a políticas públicas que mejoren la calidad de vida de la ciudadanía (Estudio de Comunicación, 2018, p. 7).

Como se evidencia, la acción típica de este tipo de delitos se encuentra en constante cambio, conforme las tecnologías dan paso a la desinformación o bien, los individuos se permiten tergiversar situaciones o hechos y tienen un público que cree la falsedad e incluso ayuda en su difusión, en algunos casos porque se identifican con su propia forma de pensar o actuar.

2.8.3.1.4 Otros aspectos de relevancia jurídico-penal. El artículo 236, establece penas de tres a seis años por difundir información falsa y establece tres escenarios: medios electrónicos, informáticos y telecomunicaciones; y limita el bien jurídico patrimonio, a nivel del sistema financiero y sus usuarios. Entonces, alguien que utiliza, por ejemplo, una red social para difundir información falsa de una persona dañando su imagen, honor, o dignidad, ¿no será sujeto activo de este artículo en particular?, lo que sin lugar a dudas crea un vacío en la tipicidad; a este tipo penal le hace falta alcance.

Los términos que se utilizan en el artículo 236, referidos a la tecnología, tienen cierto grado de amplitud y complejidad. En primer lugar, "medio electrónico", la RAE lo define como: "Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones, incluyendo cualesquiera redes de comunicación abiertas o restringidas como internet, telefonía fija y móvil u otras" (RAE, 2014).

Como se evidencia, el concepto de medio tecnológico es sumamente amplio y da paso a interpretaciones diversas al tipificar o juzgar un delito de difusión de información.

"Al hablar de medios "informáticos", pareciera referirse al computador como tal, pues ese término en particular se utiliza, para aludir a aquellos medios que se caracterizan por estar configurados en un software y articulados mediante el ordenador" (López, 2006, citado por Licona, 2012, párr. 6) y, además, se agrega que se consideran medios informáticos: "el hipertexto, la multimedia, las presentaciones en ordenador, los vídeos interactivos" (Licona, 2012, párr. 9), esta definición sitúa el área de acción a un ordenador específico, en un lugar determinado. En todo caso, debería hablarse de medios telemáticos, en los que sí se incluye, por ejemplo, el internet.

Otro aspecto destacable en el artículo 236, es que establece el daño en la distorsión o perjuicio de la seguridad y estabilidad del sistema financiero, lo que limita en gran forma su nivel

de acción y deja de lado que la difusión de información falsa, puede atentar contra otros derechos y ocasionar daños tanto a nivel individual como a nivel social. Las llamadas noticias falsas, hoy en día, son comunes en las redes. Para ello, solo hace falta ver lo que sucedió en los inicios de la pandemia Covid-19, cuando este tipo de contenido provocó inestabilidad y desorden. Sin embargo, la redacción de este artículo 236 parece dejar fuera ese tipo de acciones.

Ahora bien, el paradigma de la forma en que llegaban las noticias ha cambiado: antes el público confiaba en la información brindada por los diferentes medios televisivos y de radio; actualmente, cualquier persona puede ser comunicadora de una noticia.

Esto es relevante porque el derecho a la libertad de expresión e información tiene un roce con el artículo aludido, en virtud de que cualquier persona se podría ver en un proceso penal por haber difundido información falsa a través de los medios electrónicos y que, con ello, distorsionaran o causaran algún perjuicio a la seguridad y estabilidad del sistema financiero o a sus usuarios. Para el abordaje de este delito, se requiere conceptualizar, en primera instancia, qué se considera como difusión de información falsa, también llamada *fake news*, desinformación, bulo o posverdad, según el estudio o la región en la que se utilice y la facilidad con la que se difunde.

Tras el análisis de los tres delitos, se puede ver que existen elementos que deben mejorarse o corregir; uno de los principales es la terminología de estos tipos informáticos. Al respecto, Lemaître (2010) indica que:

> Los actuales delitos informáticos del Código Penal Costarricense, son reflejo de una mala práctica legislativa, desconocimiento del tema y una respuesta apresurada de un problema emergente, el cual no recibió el proceso serio de creación jurídico-informático que se requería, los tipos penales presentan errores de forma, fondo y de desconocimiento de la

> terminología informática consignada en los artículos, lo cual agrava la protección real de este tipo de delitos (p. 211).

En la misma línea, en relación con el papel fundamental de los legisladores y la especificidad tan necesaria en el tema de delitos informáticos y su subsecuente actualización, Lemaître (2020) aporta que:

> La Asamblea Legislativa, en primer lugar, tendrá que llevar a cabo proyectos bajo la concepción de leyes especiales sobre delitos informáticos, los cuales se desarrollarán de manera prudente, considerando el marco real de las amenazas informáticas existentes y la interrelación entre el derecho y la informática, la cual debe concurrir al crear estas figuras delictuales. De igual manera, se hace necesaria una constante actualización y revisión del área al ser un tema cambiante. Por otro lado, la legislación procurará seguir el ritmo vertiginoso de nuevos delitos informáticos, además buscar adherirse a los acuerdos internacionales que brinden instrumentos de colaboración a nivel mundial. (pp. 233-234).

La ciberdelincuencia está en constante cambio, por lo que la Asamblea Legislativa y sus dependencias deben comprometerse con la lucha decidida y actualizada. Para ello, se requiere la atención a la normativa que rige estos delitos y procurar que exista una tipicidad adecuada y clara, que responda a las necesidades y asegure procesos legales en tiempo y forma, acorde con los delitos que persigue.

CAPÍTULO III: SELECCIÓN DEL MÉTODO

3.1 Enfoque de la investigación

El presente estudio se realizará bajo un enfoque cualitativo, como tal, se pretenden revelar el significado que tienen los fenómenos investigados, en la mente de los sujetos. Se realiza una investigación participativa, por medio de las entrevistas de respuesta abierta, que se fundamentan en la información recopilada y pretende la observación de comportamientos naturales, los sujetos participantes darán sus puntos de vista y respuestas, basados en experiencias en el campo tanto del derecho como de la informática.

Se parte de una mirada holística al objeto de estudio que responde a una cultura en particular, la del ejercicio del derecho, y a la experiencia en el campo legal e informático. Sobre este método de investigación, Taylor y Bogdan (2000), determinan que "La frase metodología cualitativa se refiere en su más amplio sentido a la investigación que produce datos descriptivos: las propias palabras de las personas, habladas o escritas, y la conducta observable" (p. 7).

Por otra parte, esta investigación "se interesa por captar la realidad social a través de los ojos de la gente que está siendo estudiada, es decir, a partir de la percepción que tiene el sujeto de su propio contexto" (Bonilla & Rodríguez, 1997, p. 84).

En este sentido, Bonilla y Rodríguez (1997) sugieren que el investigador interpreta el mundo en el que se desenvuelven los individuos consultados. El proceso de indagación es inductivo y el investigador interactúa tanto con los participantes como con los datos, busca respuestas a preguntas que se centran en la experiencia social, cómo se crea y cómo da significado a la vida humana.

3.2 Método de la investigación

Para el presente trabajo investigativo, se ha seleccionado la investigación de tipo descriptiva, pues se considera que responde a los objetivos específicos propuestos, dado que se busca indagar sobre las características y rasgos del delito informático en la sociedad costarricense y la efectividad del sistema jurídico penal, desde el punto de vista de los operadores del derecho.

En cuanto a las características descriptivas de una investigación, afirman Hernández, Fernández y Baptista (2006) que se "busca especificar propiedades, características y rasgos importante de cualquier fenómeno que se analice. Describe tendencias de un grupo de población" (p. 103).

Por su parte, el concepto de método se refiere a un proceso de planificación de carácter tanto epistemológico como teórico-metodológico, el cual involucra una serie de decisiones concernientes a los procedimientos destinados a la recolección, procesamiento y análisis de datos, dentro de las cuales se encuentra la selección de las técnicas y el diseño de los instrumentos de investigación (Mata, 2020). A partir del método, se pretende recolectar la mayor información posible para obtener los insumos necesarios que arrojen datos importantes para el trabajo investigativo.

Como explica Quintana (2006), el método de investigación cualitativa se inicia con un acercamiento previo a la realidad que va a ser objeto de análisis

> (…) cuyo objetivo es documentar la realidad que se va a analizar y planificar el encuadre más adecuado para realizar la investigación, se realiza a través de dos acciones básicas: 1. Revisar toda la documentación existente y disponible sobre dicha realidad 2. Observar con antelación la realidad a investigar y, en ocasiones, entrevistar a "informantes clave". Por documentación, se entiende cualquier tipo de registro anecdótico archivado, es decir: actas,

> correspondencia personal o institucional; memorias, registros fotográficos, fílmicos o magnetofónicos; o cualquier otra evidencia material, que permita reconstruir y contextualizar el proceso, fenómeno o realidad objeto de análisis, previo al diálogo y la interacción directa con el grupo o persona participantes en el estudio (p. 52).

Se infiere que el método cualitativo se enfatiza en analizar y documentar la información con base y con enfoque en las cualidades de la pesquisa realizada.

3.3 Fuentes de la investigación

Las fuentes del estudio serán los recursos utilizados para obtener información, ya sea de manera directa, como las entrevistas, o bien, indirecta como el análisis de la jurisprudencia.

La selección de las fuentes es clave para la obtención de datos claros y reales. La fuente primaria del trabajo actual son diez profesionales en derecho y dos en informática. Al respecto, se hace la salvedad que el entrevistado Roberto Lemaitre, posee conocimientos amplios en ambas áreas.

Se utiliza información recopilada de las entrevistas realizadas y de la jurisprudencia que se considera oportuna por responder a los fines de la investigación.

Dentro de las fuentes secundarias, se consideran las utilizadas para la elaboración del marco teórico desarrollado.

3.4 Unidades de análisis

Una vez recopilada la información de las entrevistas aplicadas a los operadores del derecho y a los profesionales en informática, se identifican once unidades de análisis para realizar el contraste de opiniones y aportes de los sujetos consultados. Estas unidades responden a los objetivos del trabajo investigativo:

- Concepto de ciberdelito o delito informático.

- Perfil del delincuente.
- Delitos más comunes en Costa Rica.
- Identificación del sujeto activo.
- Identificación del sujeto pasivo.
- Problemas al afrontar un proceso judicial.
- Terminología de los delitos informáticos.
- Preparación desde las universidades en materia de delitos informáticos.
- Recomendaciones para los procesos en materia de delitos informáticos.
- Tipicidad de los delitos informáticos.
- Posición de la población costarricense sobre los delitos informáticos.

3.5 Instrumentos

Se definen las técnicas y los instrumentos de recolección de datos. Para este fin es necesario tener en cuenta el enfoque desde el cual se plantea la pesquisa, el tipo de información que se pretende captar en relación con las características de la fuente o fuentes y el tiempo del que se dispone para todo el proceso.

En cuanto a la perspectiva del enfoque, en las investigaciones de tipo cualitativo se buscará que las técnicas para obtener y generar información respondan a un encuadre particular, derivado de las características de cada contexto, circunstancia, persona o grupo, más que a un proceso de estandarización u homogenización de estas (Quintana, 2006, p. 60). Asimismo, existen diversas técnicas cualitativas que pueden aplicarse al campo de la investigación, como la entrevista a profundidad y el estudio de caso; ambos se describen a continuación.

3.5.1 Entrevista en profundidad.

La entrevista es una herramienta habitual en las investigaciones de tipo cualitativo, ya que permite, como explica (Amaia Farias [et al], 2016) conocer "la perspectiva de los sujetos; comprender sus percepciones y sus sentimientos; sus acciones y sus motivaciones. Apunta a conocer las creencias, las opiniones, los significados y las acciones que los sujetos y poblaciones le [sic] dan a sus propias experiencias" (p.19)

Por su parte, la entrevista cualitativa permite recopilar información detallada en vista de que la persona que informa comparte oralmente con el investigador aquello concerniente a un tema específico o evento acaecido en su vida. Como lo explican Fontana y Frey (citados en Vargas, 2012), "la entrevista cualitativa permite la recopilación de información detallada en vista de que la persona que informa comparte oralmente con el investigador aquello concerniente a un tema específico o evento acaecido en su vida" (p.123)

Es así que, a través de la entrevista, se recolecta información suficiente para obtener los insumos necesarios para el trabajo de investigación. Por las características de los sujetos elegidos como grupo para entrevistar, en este caso, profesionales en derecho e informática, se infiere que los datos que se obtendrían permitirán un mayor y mejor conocimiento del tema que se desarrolla, a saber, la especificidad de los delitos informáticos en Costa Rica.

Dentro de los tipos de entrevistas que se proponen, se ubican la estructurada y la no estructurada. Varios autores, entre ellos, Lucca y Berrios (2003), (citados en Vargas Jiménez, 2012), indican que, en la entrevista estructurada, todos los cuestionamientos son respondidos por la misma serie de preguntas preestablecidas, con un límite de categoría por respuesta. Así, en este tipo de entrevista, las preguntas se elaboran con anticipación y se plantean a las personas participantes con cierta rigidez o sistematización; una crítica que se señala es que puede parecer

demasiado formal. Además, se supone que se formula la misma pregunta a los participantes, para entonces comparar la información obtenida; esto permite que las respuestas a esas preguntas se puedan clasificar y analizar con más facilidad.

En cuanto a la entrevista no estructurada, señala Vargas (2012) que "destaca la interacción entrevistador- entrevistado el cual está vinculado por una relación de persona a persona cuyo deseo es entender más que explicar" (p. 127) Para este tipo de entrevistas agrega la autora que es recomendable la formulación preguntas abiertas, claras, únicas, simples que deben responder al tema de investigación. Del mismo modo, explica Vargas (2012) que "la entrevista no estructurada puede proveer una mayor amplitud de recursos con respecto a las [sic] otros tipos de entrevista de naturaleza cualitativa". (p.126)

Para efectos de este trabajo investigativo, se formulan entrevistas estructuradas con base en unidades de análisis específicas, sin embargo, a cada sujeto de la muestra, se le formulan preguntas abiertas, para obtener explicaciones con base en la experiencia de cada sujeto, todas sobre la línea de la investigación.

En el instrumento propuesto se cuestiona sobre la definición de ciberdelitos, identificación de los sujetos pasivos y activos, la tipicidad de los delitos informáticos y su normativa, así como problemas al litigar en los casos específico de la ciberdelincuencia. Estas entrevistas son dirigidas a grupos expertos tales como jueces, fiscales, defensores y abogados litigantes, así como a ingenieros en informática (ver Anexo N.º 1).

Se considera fundamental la opinión y la experiencia de tres defensores públicos, dos litigantes, dos jueces, dos fiscales y dos ingenieros en informática; además, se cuenta con el aporte de un especialista en ambos campos; es decir, un abogado con maestría en informática.

Posteriormente, se procederá al análisis individual de cada entrevista y luego, se contrastan los resultados con base en las unidades de análisis establecidas en el marco metodológico.

3.5.2 Estudio de caso mediante el análisis de jurisprudencia.

El análisis jurisprudencial es un espacio de reflexión que se da entre un investigador o intérprete, frente a un grupo de sentencias emitidas por las altas cortes o instancias menores, dentro de la jerarquía de producción de jurisprudencia, en determinado contexto judicial.

Dicho análisis indagará por la argumentación que hacen los jueces frente a determinado problema que ha sido propuesto por el investigador y frente al cual se busca encontrar respuestas en forma de fallos judiciales. Estos permitirán al investigador sacar conclusiones acerca de cómo se está resolviendo tal problema por parte de los jueces. Sin embargo, es importante indicar que no existe un único modo de realizar dicho análisis. Las propuestas metodológicas son siempre herramientas importantes que permiten acercarse al objetivo propuesto, pero no hay tan solo una y es dable al investigador encontrar la que se acomode mejor a la búsqueda de respuestas frente al problema que se plantea (Coral, 2012, p. 19).

Mediante este sistema de análisis de jurisprudencia, se espera obtener información relevante en cuanto al tratamiento que le ha dado la administración de justicia a casos específicos en relación con los delitos informáticos. La argumentación por parte de los jueces, en estos delitos, permitirá conocer de primera mano cómo se fundamenta cada caso en específico, de una materia aún complicada, como son los supracitados delitos informáticos.

3.6 Proceso para la recolección y análisis de datos

Para efectos de esta investigación se realiza, en primera instancia, una revisión de bibliografía que permite aclarar los conceptos clave y las diferentes posturas teóricas sobre el abordaje de los delitos informáticos.

Posteriormente, se aplican entrevistas de respuesta abierta a los sujetos seleccionados, con las cuales se pretende realizar un análisis de las variables consideradas para esta investigación. Para ello, se identifican, en al apartado de análisis de datos, las ideas y los argumentos considerados importantes en cada uno de los casos y se contrastan los diferentes puntos de vista, para identificar concordancias y diferencias en el abordaje del tema.

Seguidamente, se analizan las jurisprudencias de la Sala Tercera y los Tribunales de Apelación de Sentencia Penal del año 2019 y 2020 (ver Anexo n°2). De estos pronunciamientos se extraen aportes relevantes para evidenciar el abordaje que, en materia penal, se ha realizado en Costa Rica, en relación con los delitos informáticos procesados.

En cuanto a la jurisprudencia, se analizarán las siguientes resoluciones para los fines de la propuesta investigativa:

1) Resolución numeral 01076-2020. Sala Tercera.

Expediente: 13-001603-0042-PE con fecha de resolución: 28 de agosto de 20202.

Clase de Asunto: Recurso de casación.

2) Resolución numeral 00494-2020. II Circuito Judicial de San José.

Expediente: 16-003520-0059-PE con fecha de resolución: 26 de marzo de 2020.

Clase de Asunto: Recurso de apelación penal.

3.7 Selección de la muestra

Se trabajará tanto con teorías como con datos aportados por los entrevistados y la información de la jurisprudencia. La selección de los participantes se dio por conveniencia, de acuerdo con el perfil requerido para el tema de investigación.

Se consideran, para el trabajo investigativo, dos abogados litigantes, expertos en delitos informáticos, para conocer la forma en que desarrollan sus casos, cuando alguno de sus clientes se

ven inmersos en estos delitos. Además, siete profesionales del Derecho Penal, defensores, fiscales y jueces, para conocer todo lo concerniente al desarrollo de los procesos penales en materia de delitos informáticos. Por último, se analizan los aportes de dos ingenieros en Informática y de un licenciado en Derecho con maestría profesional en Computación e Informática.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

Para efectos de esta investigación, se formuló un instrumento de entrevista con diez preguntas básicas (Ver anexos n°2), en las mismas se propuso evidenciar las unidades de análisis especificadas en la selección del método. En este capítulo, se analizan cada una de las respuestas obtenidas de los entrevistados y, posteriormente, se contrastan aspectos relevantes sobre las ideas aportadas. Se entrecomillan frases o información importante tomada de forma textual de las entrevistas aplicadas. También se realiza el análisis de la jurisprudencia especificada para el estudio y se contrasta con las opiniones emitidas por los sujetos consultados.

4.1 Personas Defensoras públicas

4.1.1 Licenciado Juan Pablo Rojas Arias.

Cuando se le consulta sobre qué es un ciberdelito o delito informático, el participante afirma que es aquel en el que intervienen medios informáticos y que supone el uso de algún dispositivo electrónico para cometer un delito, respuesta que corrobora el conocimiento básico del término en análisis.

Como se ha analizado anteriormente, varios autores consideran que un ciberdelincuente tiene conocimientos previos del área informática, por lo que se consulta al entrevistado el perfil de quien comete un delito de este tipo. Al respecto, el licenciado Rojas, no considera que exista un perfil definido, pues cualquier persona podría llegar a cometer un delito informático. Incluso, ejemplifica diciendo que “se tienen indigentes que pasan por delitos informáticos simple y sencillamente porque se les abrió una cuenta y se les depositó un dinero” (Rojas, 2020).

Se le consulta al entrevistado qué delitos informáticos son más frecuentes, según su experiencia, a lo que señala dos en particular: el fraude y la difusión de pornografía en redes sociales, al menos en la zona de San José y Cartago.

Quizás uno de los aspectos más delicados y difíciles, en lo que respecta a la aplicación de la ley en delitos informáticos, es la determinación del sujeto activo, el entrevistado concuerda con esa idea; señala que se cometen errores cuando se castiga al último eslabón de la cadena del delito, esas personas que, fueron engañadas, y

> nunca llegan a manipular un sistema, nunca llegan a extraer la información de la parte ofendida, ni siquiera saber cuál fue el origen de ese dinero y eso ha generado que tengamos una taza alta de delitos pero que realmente nunca han determinado quien fue la persona, cuál fue el medio que se utilizó, cuál computadora se utilizó (Rojas, 2020).

Menciona el participante que, aun cuando OIJ y el Ministerio Público logran identificar a quien extrajo la información, no existe estafa informática,

> porque la información con la que se está accediendo es una información real que se extrajo por medio de un engaño, pero la llave que se está utilizando para ingresar a los sistemas informáticos es la llave correcta que cualquier persona utilizaría (Rojas, 2020).

Termina su argumentación indicando que no hay estafa informática si se utilizó información verdadera.

Como se observa, parece evidente que existen complicaciones para afrontar un proceso judicial en este tipo de delitos, por lo que se le consulta a Rojas, cuál es el mayor problema; sin embargo, en su respuesta, establece que, para efectos de una defensa, más bien se llega a sobreseimientos, pues siempre hay justificación viable.

El entrevistado recalca que lo que existe es una presión internacional por lograr resolver los casos derivados del cibercrimen, pero que, en muchos casos, tras la investigación

> en un proceso apegado el derecho, apegado a elementos probatorios reales, apegado a un análisis objetivo del juez casi que ninguno debería llegar a la etapa de debate, sin embargo, hay una presión social que hace que algunos lleguen a juicio (Rojas, 2020).

Por lo aportado en los argumentos, se observa que el participante considera que no existen pruebas o procesos suficientes para juzgar esos delitos adecuadamente.

Al cuestionar más específicamente sobre los principales problemas o impedimentos para poder procesar a una persona en delitos informáticos, Rojas señala que ni el OIJ, ni el Ministerio Público, ni las entidades bancarias tienen la preparación adecuada para detectar inclusiones fraudulentas o bien identificar a los culpables. Si se llega a evidenciar el fraude, es porque la víctima detecta movimientos en su cuenta bancaria y presenta el reclamo, pues existe, según puntualiza, "ausencia de herramientas para la detección inmediata" Rojas (2020) que, conjugado con la "reacción tardía que tiene el OIJ" Rojas (2020), impiden el procesamiento adecuado del delito como tal.

También se consulta si la terminología del tipo penal, al hablar de *phishing, hardware, software*, genera algún problema. El entrevistado únicamente menciona el *phishing,* y establece una definición estándar del vocablo como la "persona que pone el anzuelo para que la víctima caiga" (Rojas, 2020). Cabe evidenciar la necesidad de que, al tratarse de delitos especializados, deban utilizarse términos de informática, "pero a nivel de tipos penales la determinación del delito debió hacerse más amplia" (Rojas, 2020). Concluye su respuesta estableciendo que sí existe un problema con la terminología, pues "ha generado que conductas que son de la normalidad, conductas que podrían encuadrar en otros tipos penales se agarren y se metan ahí para tener un circulante de delitos informáticos, cuando creo que no son delitos informáticos" (Rojas, 2020).

Se consulta al entrevistado si se requiere más preparación en el tema de delitos de esta índole y se obtiene una respuesta afirmativa. Se percibe un argumento de obligatoriedad para un abogado, quien debe capacitarse según la rama de aplicación del derecho en la que se especializa, sin dejar de lado que, el Colegio de Abogados debería impulsar iniciativas, aunque es evidente para Rojas que, "la especialización tiene que venir de la motivación y de la dedicación que cada profesional tenga" (Rojas, 2020).

Ante este panorama de los delitos informáticos y su penalización, al entrevistado se le solicitan recomendaciones para mejorar y, aunque al principio señala que, como defensor, no le interesa que mejore pues las falencias las utiliza para defender a sus clientes, es claro en indicar que se requiere una

> alianza fuerte del OIJ con las entidades bancarias en donde la posibilidad de determinar la sustracción de dineros casi que se dé inmediata, seguidamente, la especialización de equipos en el OIJ y la capacitación para las personas que vayan a trabajar en ese tipo de delitos (Rojas, 2020).

Del mismo modo, indica algunos aspectos propiamente técnicos para monitoreo y rastreos de usuarios.

Finalmente, se cuestiona sobre los problemas de los tipos penales. El participante argumenta que "hicieron la figura penal para tratar de encuadrar conductas en esa figura penal y no definir una conducta que ya estaba ocurriendo y tipificarla" (Rojas, 2020). Además, postula que actualmente se trata como estafa común y, si se utiliza la clave que el usuario facilitó, no existe intromisión errónea de datos falsos. El problema radica en que se incluyeron conductas normales de estafa dentro del delito informático como tal. Rojas argumenta que deberían "perseguir las

intromisiones erradas que se hagan en sistemas [pues] son estas páginas falsas que extraen la información del usuario donde podría darse un delito de estafa informática" (Rojas, 2020).

El entrevistado cierra su aporte indicando que, "no se está utilizando el tipo penal como debería de utilizarse" (Rojas, 2020), lo que sugiere una falta de tipicidad del cibercrimen.

4.1.2 Licenciado Francisco Cerna.

Ante la sobre la definición de ciberdelito o delito informático, el participante, considera que se trata de una "acción en contra de algún sistema informático que cause algún perjuicio patrimonial" (Cerna, 2020).

En relación con el perfil del delincuente informático, establece que "son personas que conocen sobre la materia informática" (Cerna, 2020), sin la necesidad de tener estudios específicos, pero que sí puedan manipular sistemas o programas y su vulnerabilidad.

Con base en lo expresado, se consulta si, en los casos de estafas que se han procesado, los imputados son ingenieros informáticos o no. Al respecto, se obtiene una respuesta negativa, pues son personas con "conocimientos empíricos o talento incluso innato" (Cerna, 2020), que les permite vulnerar los sistemas.

Se consulta al entrevistado cuáles son los delitos más comunes o que llevan a tribunales, a lo que responde que son los fraudes o estafas informáticas, generalmente por tarjetas, y agrega que se induce al error a la víctima con ayuda de "*frentiadores*" (personas que prestan sus cuentas, con o sin conocimiento, para los depósitos). Estos se convierten en los "perseguidos penalmente" (Cerna, 2020), al ser los rostros tras la estafa.

Se cuestiona, entonces, según su experiencia, cuáles son los delitos informáticos más frecuentes. El entrevistado explica que son los cometidos mediante "la impericia o falta de cuidado

de las personas" (Cerna, 2020), quienes se convierten en víctimas de *hackers* y sufren retiros de dinero de sus cuentas.

En relación con los sujetos activos y la dificultad para identificarlos, Cerna (2020), argumenta que son delitos tripartitos, en los que participa quien llama y extrae la información; el *hacker*, que realiza lo concerniente a informática; y la persona *frentiadora*, que recibe en su cuenta el dinero. Agrega que no se tiene la tecnología necesaria para la identificación de los infractores.

Ante la consulta de cuál es el mayor problema para afrontar un proceso judicial en estos delitos, el entrevistado indica que es "la imposibilidad de acreditar la forma dolosa de que la persona retiró con conocimiento de hecho el dinero" (Cerna, 2020), pues faltan elementos probatorios; a no ser que, en la indagatoria, se determine que se prestó la cuenta como un favor para un tercero. Este tipo de procesos, explica, continúan más por un tema estadístico, pero la defensa, puede demostrar "que no existía ningún tipo de conocimiento o voluntad para los efectos de la realización de ese hecho delictivo" (Cerna, 2020), lo que facilita el proceso para la persona acusada.

En este panorama, se consulta por los principales obstáculos para procesar penalmente a los delincuentes informáticos, es decir a los ingenieros, a la gente que está en las computadoras. El participante, reitera que, en Costa Rica, no hay un sistema policial o unos peritos que puedan determinar qué equipos informáticos, dirección IP o correos electrónicos, se utilizaron y, mucho menos, llegar al *hacker* involucrado.

Desde esa óptica, los abogados se deberían preparar en materia de delitos informáticos, idea que asevera Cerna, al indicar que, "el derecho es una ciencia social" (Cerna, 2020) y, como tal, debe evolucionar con los cambios y actualizarse.

Posteriormente, se le solicita al entrevistado su opinión sobre qué se puede hacer para mejorar en relación con los delitos informáticos; él expone tres argumentos: 1) crear cultura en las personas, para que no faciliten información de sus cuentas bancarias; 2) dotar al OIJ de peritos aptos; 3) prevenir y realizar buenas investigaciones, que sean efectivas, y no solo por estadística. Sobre el tipo penal y su tipicidad, el entrevistado prefirió no responder, pues afirmó no tener el dato a su alcance al momento de la entrevista.

Finalmente, se consulta si existe algún problema a nivel de investigación o del mismo proceso en cuanto al lenguaje que se utiliza en la informática, por ejemplo: *phishing*, *hardware*, *software, hacker*. Cerna responde que, efectivamente, debe existir una preparación, no como profesional en informática, pero sí suficiente para realizar el abordaje. También, señala que se puede acudir a "peritos o consultores técnicos" que ayuden en la comprensión de la materia.

4.1.3 Licenciado Joffre Montero Zúñiga.

En relación con la pregunta sobre qué es un delito informático, el licenciado explica que es cuando se vulnera un sistema informático y cuyo bien jurídico son "datos o información" (Montero, 2020). Además, agrega que esos datos pueden estar en "contenedores magnéticos, contenedores de almacenamiento, memorias, discos duros, plataformas de información" (Montero, 2020).

Sobre el perfil del delincuente, se hace la salvedad de que, por un lado, está la persona que resulta imputada: "usualmente el perfil de estas personas es de baja escolaridad, urbano-marginales, quienes lo hacen a cambio de algún tipo de beneficio de dinero, en ocasiones pueden que sepan que es un delito, en otras no, inclusive son engañados" (Montero, 2020); por otro lado, las "personas que tienen una capacitación en el manejo de sistemas de información" (Montero,

2020) y agrega que “los hackers tratan de no dejar ningún rastro tanto informático como físico” (Montero, 2020).

Ante esta respuesta, se consulta sobre la dificultad de rastrear a quien comete el delito desde el computador. El entrevistado explica que una persona que falsifica la página de una entidad bancaria podría ocultarse tras una dirección IP en otro país, lo que hace imposible verificarla y, al final, solo se identifica al tercero, cuya cuenta fue utilizada para extraer el dinero.

En cuanto a los delitos más frecuentes, concuerda con otros participantes en cuanto a que la estafa informática es la más común.

Sobre los sujetos activos, Montero explica que es muy difícil identificar a quienes están detrás del delito, ya que suelen utilizar técnicas que los dejan en el anonimato. El uso de una VPN (*Virtual Private Network*, tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet) y el tránsito en la web oscura, facilitan la ciberdelincuencia y los sujetos activos se vuelven casi inidentificables, difíciles de rastrear.

Como principales obstáculos al procesar penalmente a los delincuentes informáticos, Montero señala que está lo que él llama “la anonimización” (Montero, 2020), la posibilidad que tienen de anonimizar las direcciones IP y borrar todos los rastros; además, señala la dinámica compleja de los delitos, la internacionalización al existir la globalidad de los datos. Esto agregado a que la policía de investigación “no tiene las herramientas tecnológicas para poder desenmascarar este tipo de delitos [o bien, se] quedan cortas” (Montero, 2020) ante los delincuentes. Con respecto al factor internacional, agrega que existe el Convenio de Budapest, con el que se puede acceder a información policial extranjera, pero solo en el caso de que el país esté inscrito en el convenio.

En cuanto a la terminología del tipo penal, Montero externa que no debe ser un problema, se debe estudiar lo que corresponda o acudir a un perito, pues es una obligación para establecer la figura delictiva.

Sobre la ubicación de los delitos informáticos en la normativa, se consulta si deberían estar concentrados o si funcionan como están, a lo que el entrevistado argumenta que no debería afectar donde están y señala que el problema con ello es que "los tipos penales que nosotros tenemos no son muy claros, tienen errores en términos relevantes, algunos no diferencian entre datos e información que son cosas diferentes" (Montero, 2020).

Con referencia a la necesidad de que los profesionales en derecho se especialicen en las universidades sobre temas informáticos, se argumenta que, a nivel de posgrado, sí se considera importante.

Al solicitar recomendaciones sobre el procesamiento penal en Costa Rica de estos delitos, el licenciado indica que la acción debe ser inmediata y no dar tiempo a los delincuentes para ocultar su rastro. Además, agrega que se requieren convenios internacionales para el acceso a la información, aunque medidas como esas son complicadas en plataformas como Facebook, por ejemplo.

Finalmente, con respecto a la tipicidad del delito, Montero argumenta que hay problema por la amplitud del tipo penal, como el delito de estafa informática, por ejemplo, que "contiene tantas descripciones que lo hace ser muy amplio" (Montero, 2020).

4.2 Abogados litigantes

4.2.1 Licenciado Henry Angulo Yu.

En primera instancia, ante la consulta sobre qué es un delito informático, el entrevistado explica varias posiciones de autores como Francisco Castillo; sin embargo, no establece una

definición como tal, pues considera que el término es muy complicado de definir, aunque hace hincapié en que la estafa informática es uno de ellos.

Sobre el perfil del delincuente informático, el entrevistado indica que, desde un punto de vista generacional, se podría situar en rangos desde los 12 hasta los 50 años o bien, personas nacidas en los años setenta. Otro aspecto es la profesión; se catalogaría como una persona inteligente, que posee automotivación para violar sistemas informáticos y la seguridad de las entidades como bancos. Argumenta, también, que son personas con habilidad y que manipulan a terceros para realizar el ilícito.

En cuanto a los sujetos activos, explica Angulo, que es casi imposible identificar al autor intelectual, por las facilidades del Internet. De esta forma, quien "paga los platos rotos" (Angulo, 2020) es el partícipe que si se identifica.

Para el entrevistado, el problema a la hora de afrontar un proceso judicial es identificar a los autores; además, el OIJ tiene recursos limitados, pues, aunque se capacita a su personal, el delito informático está en constante cambio. Con referencia a la óptica procesal, agrega que "hay bastante desconocimiento de los operadores jurídicos" (Angulo, 2020). Rescata, además, que debe existir mayor capacitación y especialización y que, en el ámbito operacional, se debe priorizar esa política criminal.

Sobre procesar penalmente a un delincuente, el entrevistado aclara que únicamente ha podido llevar a juicio a quien saca el dinero producto del fraude, no así al autor del delito.

Al cuestionársele acerca de la terminología, el participante explica que se utilizan muchos anglicismos que, a la hora de su traducción, pierden su significado.

Por otro lado, cuando se le consulta sobre la estafa informática en el 216 y 217bis, es claro en indicar que la dificultad está en la definición misma, porque es muy amplia y "todo delito calzaría mientras allá una computadora involucrada" (Angulo, 2020).

En cuanto a si incluir o no una asignatura sobre delitos informáticos en la formación de estudiantes de derecho, Angulo expresa que es importante, pero como optativa o, al menos, para comprender el asunto.

Al cuestionar al entrevistado sobre qué recomendaciones aportaría para procesos de este tipo de delitos, este señala: la capacitación, la mejora del recurso humano y del material y la clasificación adecuada de lo que ya se tiene en el código.

Cuando se le cuestiona en relación con el artículo 230 del Código Penal, sobre la suplantación de identidad, el entrevistado expone que este delito es "el pan de cada día" (Angulo, 2020), solamente que las víctimas prefieren reportar en la red social (el perfil falso, por ejemplo), que denunciarlo. Por último, hace referencia al artículo 236 sobre difusión de información falsa, cuyo delito tiene posibilidad de viralizarse, y puede causar daños graves a la víctima.

4.2.2 Licenciado Adalid Medrano Melara.

En una primera consulta, se solicita al participante su definición de delito informático. Este indica que es "vulnerar la confidencialidad, la integridad y la disponibilidad de los sistemas o datos informáticos o contra la autodeterminación informativa o identidad en medios electrónicos" (Medrano, 2020); para él, al definirlo de este modo, se incluye la suplantación y la violación de datos personales.

Por la respuesta obtenida, se le solicita al entrevistado una explicación de delitos informáticos. Explica que la estafa informática es el que se encuentra más presente en la realidad costarricense y que se cometen otros delitos, en el *iter criminis*, como la suplantación de páginas

electrónicas o un sitio de Internet. Del mismo modo, se da la suplantación de identidad y la instalación o la propagación de programas informáticos maliciosos. Todos esos caminos facilitan la comisión del fraude.

Agrega, además, que el delito de violación de datos personales, lo que él llama "el mercado negro de datos personales de los costarricenses" (Medrano, 2020), facilita obtener información para que el usuario crea que está tratando con la entidad bancaria real. Añade que el facilitador del delito informático, aun sabiendo las intenciones fraudulentas, alquila los servidores o los correos electrónicos para cometer el delito. La complejidad de la estafa informática es mucha, incluso con una "tarjeta SIM" o con "SINPE móvil" se puede generar el fraude.

Con referencia al perfil del ciberdelincuente, establece Medrano que cualquiera puede serlo; desde el especialista en informática, hasta un usuario de una computadora en la que se ha dejado abierto un correo o una página personal sin una clave que la proteja. En este caso en particular, si se toman los datos y se copian o se venden, se cae en el delito de violación de datos personales, sin requerir mayor preparación técnica. Ante ese panorama "cualquiera puede ser víctima, pero cualquiera puede ser victimario también" (Medrano, 2020).

Cuando se consulta el perfil del sujeto pasivo, Medrano afirma que cualquier persona puede ser sujeto pasivo solo con tener un medio informático. En el caso de la estafa, suelen ser, en un 95%, personas con poco conocimiento en informática, aunque nadie se salva de estos delitos si no tiene protocolos para protegerse. El entrevistado agrega que, en la etapa escolar, debe enseñarse sobre ciberseguridad; sin embargo, no todas las personas tienen acceso a un sistema educativo formal, pese a que la mayoría interactúa en medios tecnológicos. Se requiere educar a toda la población, pues actualmente no basta con claves personalizadas. La firma digital certificada es una alternativa de seguridad, pero no todos pueden acceder a una.

Al consultarle sobre los delitos más comunes, Medrano cita cinco: estafa informática, suplantación, difusión de información falsa, violación de correspondencia y seducción o encuentro con menores por medios electrónicos.

Seguidamente, se le cuestiona sobre la dificultad de identificar a los sujetos activos y se exponen dos variables; por un lado, cuando el delito lo comete un profesional, generalmente es más difícil de identificarlo, por las herramientas que utilizan para protegerse. Por otro lado, si el delito lo realiza una persona no especializada, se pueden identificar evidencias digitales para vincularlo al hecho denunciado.

También se cuestiona a Medrano sobre el mayor problema en un proceso judicial por delitos informáticos y explica, por etapas, los problemas que se dan. Cuando se denuncia, no hay personal capacitado sobre esa materia y puede llegar incluso a obviarse la denuncia y archivarla. Otro aspecto es el tiempo que se dura en entregar la información a las autoridades; en este punto, hace alusión al proyecto de Ley 21.187, que pretende reducir los tiempos de entrega por parte de los proveedores de internet. Por último, señala la falta de preparación de los fiscales o la carencia de herramientas tecnológicas que dificultan el tratamiento de evidencias digitales.

Con base en la experiencia, se le consulta sobre los impedimentos para procesar penalmente a los ciberdelincuentes. Medrano señala que, principalmente, son problemas de carácter probatorio, en la recopilación de evidencias digitales suficientes y el conocimiento de jueces y fiscales en el tema para valorar esa evidencia.

Al preguntarle si los abogados deben especializarse en materia de delitos informáticos desde la universidad, es enfático al señalar que debería impartirse Derecho Informático como materia, debido a que los delitos informáticos van en aumento y cambio constante. Al respecto aporta que el “Colegio de Abogados y Abogadas está haciendo grandes esfuerzos a través de

comisiones como la de derecho informático" (Medrano, 2020) y ha iniciado la "Innovación Regulatoria que va a analizar todos estos temas, porque es una necesidad que tenemos como país" (Medrano, 2020).

Seguidamente, se pregunta qué se necesita mejorar a nivel de la persecución de este tipo de delitos. El entrevistado indica que se debe generar una nueva política criminal; para ello, se propone la Ley 21187, cuyo objetivo es establecer estrategias contra el cibercrimen. También, se alude a incorporar nuevos tipos penales, como el acoso cibernético. Asimismo, se necesita presupuesto para atender la lucha contra este tipo de delitos, pues como explica Medrano, "se creó una sección contra el cibercrimen dentro de la fiscalía segunda llamada Fiscalía Adjunta de Fraudes y Cibercrimen" (Medrano, 2020), donde tienen más de mil casos, principalmente de estafas informáticas, pero solo tienen dos fiscales.

Finalmente, por la influencia de las redes sociales, se le consulta sobre la forma en que la población hace uso de esos medios. El participante argumenta que se requiere mayor conciencia a la hora de suministrar información, prepararse adecuadamente, informarse y no facilitar el delito, después de todo, "la ciberdelincuencia mejora con mucha más rapidez y los ciudadanos deben capacitarse con igual celeridad o quedan en indefensión" (Medrano, 2020).

4.3 Entrevista a ingenieros informáticos

4.3.1 Ingeniero Luis Diego Alfaro Alpízar.

En primera instancia, se le solicita al entrevistado su definición de delito informático y este explica que es una acción por medios tecnológicos que busca distorsionar, suplantar o robar y provoca afectación en el momento o en el futuro.

Al consultarle sobre el perfil del delincuente en estos delitos, explica que no hay un perfil, aunque supone que un atributo debe ser el conocimiento en el área informática. Asimismo, señala

que se deben tener en cuenta tres líneas de sombreros: “blanco: los que ayudan; negro, los que afectan; gris, los que no están ni a favor ni en contra y muchas veces no definen en qué parte se encuentran, puesto que pueden estar en las dos” (Alfaro, 2020). Incluso, Alfaro aporta que la denominación “*hacker*” ha cambiado de tal forma que, actualmente, se habla de “*hacker* ético” para referirse al perfil de aquellos que ayudan.

Acerca de la dificultad para perseguir a los delincuentes informáticos, explica que estos se enmascaran para ser indetectables y hay mucho desconocimiento en el área. Agrega que los usuarios no siguen recomendaciones de seguridad y eso dificulta las investigaciones.

Ante la pregunta sobre los delitos más frecuentes en Costa Rica, Alfaro señala que la más denunciada es la estafa, aunque él considera que son las distorsiones por robo de información o encriptado de datos, pero estas no se denuncian.

Con referencia a la dificultad para identificar sujetos activos, el entrevistado menciona que la informática forense es una alternativa en la actualidad, “se trabaja de la mano porque sean los mismos algoritmos los que identifiquen este tipo de sujetos” (Alfaro, 2020), añade que en seguridad informática se trabaja sobre la detección y la solución del ataque.

Al consultarle si es necesario que un abogado reciba la materia de delitos informáticos, Alfaro señala que es importante, pero, más aún, que debe impartirse informática como tal para ampliar el conocimiento.

Por último, ante la comentada dificultad para identificar a los delincuentes, explica que no es difícil, pero se requiere “técnica, experiencia y análisis de comportamientos” (Alfaro, 2020) y, principalmente, el apoyo de más especialistas.

4.3.2 Ingeniera Marisol Núñez Vásquez.

Primeramente, sobre la definición de delito informático, la entrevistada indica que es una "acción o actividad ilegal que se realiza haciendo uso de la tecnología" (Núñez, 2020). Aunado a ello, para caracterizar el perfil del delincuente, indica que puede ser cualquier persona con habilidades en sistemas informáticos o acceso a información sensible; desde un novato hasta grupos organizados.

Cuando se cuestiona acerca de los obstáculos al perseguir a los delincuentes, la participante argumenta tres razones principales: la dificultad en el rastreo de huellas digitales, la rapidez con que se ejecuta en el ciberespacio y los cambios constantes en la tecnología.

Al consultarle a la entrevistada sobre los delitos informáticos más frecuentes, esta enumera los determinados en estadísticas del OIJ como la estafa, la suplantación, la difusión de información falsa, entre otros. Sin embargo, agrega que muchos delitos no son denunciados para proteger la imagen de la víctima.

Seguidamente, se cuestiona sobre la dificultad de identificar a los sujetos activos. La participante afirma que es difícil, pues se requiere personal calificado y en el país no hay especialidades sobre el tema. Además, opina que existe un "desligue entre el profesional de ámbito legal y el de ámbito informático" (Núñez, 2020), brecha que debe acortarse para tener resultados.

En cuanto a su criterio sobre si se debe incluir la materia de delitos informáticos en la preparación universitaria de los abogados, Núñez es clara en aseverar que es necesario y no solo del delito, sino preparar a todo "el personal forense e investigador que se requiere" (Núñez, 2020).

Por último, la entrevistada explica que la dificultad para identificar a los delincuentes está en no contar con profesionales especializados que puedan "crear perfiles e identificar los patrones de conducta" (Núñez, 2020), asimismo, en carecer de recursos para hacer lo que se necesita.

4.4 Entrevista a jueces de la república

4.4.1 Licenciado Olivier Ramírez Valverde.

Primeramente, se le consulta al entrevistado, sobre qué es un delito informático. Este señala que se trata de “ilícitos cometidos mediante el uso de mecanismos electrónicos o informáticos” (Ramírez, 2020). Estos se ejecutan en contra de individuos o empresas y pueden vulnerar el patrimonio o la intimidad.

Seguidamente, se le consulta sobre qué ley regula estos delitos en Costa Rica y explica que están regulados en el Código Penal como “violación de datos personales, estafa informática, alteración de datos o sabotaje electrónico y violación de comunicaciones electrónicas” (Ramírez, 2020).

Cuando se cuestiona concretamente sobre quién comete esos delitos, el participante ofrece una respuesta directa: “cualquier persona” (Ramírez, 2020). Del mismo modo, al indagar acerca de quién es el sujeto pasivo, el entrevistado indica: “cualquier persona o entidad financiera” (Ramírez, 2020).

Ante la pregunta sobre los delitos informáticos más frecuentes, puntualiza que es la estafa informática en cuentas bancarias, en la que, mediante engaños, se utiliza a la propia víctima como instrumento del delito.

Se cuestiona a Ramírez sobre la dificultad para identificar a los sujetos activos, a lo que responde afirmativamente. Indica que es complicado saber quién efectuó el ilícito tras el medio tecnológico y que se complica obtener elementos probatorios.

Al formular el cuestionamiento relativo a cuál es el mayor problema a la hora de enfrentar un proceso judicial en esta materia, el participante señala que es, precisamente, identificar al sujeto activo y recuperar el dinero sustraído.

Se pregunta al entrevistado sobre los impedimentos u obstáculos para procesar penalmente a los delincuentes y este responde que el “ilícito se puede cometer en cualquier parte del mundo” (Ramírez, 2020), pues esto no permite determinar la identidad del delincuente.

En relación con la pregunta: ¿Considera usted que las universidades deberían incluir la materia de delitos informáticos?, responde afirmativamente. Incluso, señala que, además de la materia de delitos informáticos, debe incluirse el análisis del tipo, esto ayudaría a solventar el problema de la falta de pruebas en los procesos.

Se le solicitan a Ramírez sus recomendaciones para mejorar el procedimiento penal en la materia, a lo que explica que el Ministerio Público debe ser más efectivo en sus diligencias, solicitar levantamiento de secreto bancario y aportar estados de cuentas, por ejemplo.

Por último, se le solicita su opinión sobre el uso que hace la población del Internet, a lo que responde que son más precavidos al brindar datos; sin embargo, hay quienes siguen cayendo en los engaños.

4.4.2 Licenciado Erick Roberto Barrios Sancho.

Ante la consulta de qué es un ciberdelito, Barrios, afirma que es aquel ilícito en el que media la tecnología, donde se compromete o se afecta el patrimonio y menciona que es “vulnerar el honor o la reputación de las personas físicas o jurídicas” (Barrios, 2020).

En una segunda pregunta, el consultado señala ocho artículos del Código Penal que regulan los delitos informáticos, “numerales 217 bis, 229 bis, 229 ter, 230, 231, 232, 233 y 234” (Barrios, 2020), y resalta que estos delitos se cometen en asocio con otros. Entre los principales señala la estafa, el daño, el sabotaje, la suplantación de identidad, entre otros.

Seguidamente, explica en la tercera consulta que se comete este delito cuando una persona física dolosamente altera, suprime, daña o modifica algún sistema tecnológico y genera algún daño al bien jurídico.

Cuando se le consulta a Barrios, sobre el sujeto pasivo, que responde que este puede ser cualquier persona. Sin embargo, aclara que, generalmente, las víctimas poseen "grandes sumas de dinero en cuentas de ahorro, corrientes, valores" (Barrios, 2020) y que, al extraer claves o números de cuenta, sufren sustracción de sus bienes.

Para el entrevistado, el delito más frecuente es la estafa informática. También, indica que son frecuentes los delitos contra el honor en las redes sociales, delitos sexuales y trata de persona en el ciberespacio.

En relación con los sujetos activos, explica que el delincuente es difícil de ubicar, pues puede actuar desde cualquier parte del mundo o bien, encubierto tras un perfil falso. Agrega a esta dificultad el hecho de que las autoridades están poco capacitadas en este tipo de delitos.

En la consulta sobre es el mayor problema al enfrentar un proceso judicial, el entrevistado argumenta sobre la falta de recursos para especializar a fiscales e investigadores y obtener pruebas, pues recuerda que "la duda favorece al encartado" (Barrios, 2020).

Con referencia a impedimentos y obstáculos, establece la identificación del culpable, la prueba técnica, la falta de recursos para investigaciones, la falta de conocimientos de los acusadores y el exceso de formalismo para solicitar información; por ejemplo, el secreto bancario.

Se consulta a Barrios si las universidades deberían incluir la materia de delitos informáticos en su currículo, a lo que responde enfáticamente que sí. De hecho, lo considera imprescindible.

Al respecto de los procedimientos penales en Costa Rica, el entrevistado recomienda una modificación a la ley procesal penal que agilice trámites, "que la fiscalía y el Organismo de

Investigación Judicial tengan la facultad de pedir la información de manera más oportuna" (Barrios, 2020); con ello, se evita la impunidad, deben agilizarse los procesos, ser tan rápidos como se pueda.

Por último, sobre el uso que la población hace del Internet, señala que nota mucha confianza en la gente, que facilita las claves y cuentas, publica fotos y revela información personal, lo que facilita el delito.

4.5 Entrevista a fiscales de la república

4.5.1 Máster Carlos Arias Córdoba.

En la primera consulta, se pregunta qué considera como ciberdelito o delito informático, a lo que responde que es una acción que se realiza para ocasionar un perjuicio patrimonial antijurídico, a la intimidad y la moral en el que se utilizan medios tecnológicos.

Cuando se le pregunta cuál ley regula estos delitos, el entrevistado declara que el Código Penal y el Convenio de Budapest sobre ciberdelincuencia.

Ante la consulta de quién comete estos delitos, Arias cita lo que establece el Código Penal, en el que se menciona que se refiere a la persona que, para buscar un beneficio, utiliza un sistema de cómputo o medios informáticos.

Cuando se pregunta sobre el sujeto pasivo, el entrevistado explica que es la persona que cae en el engaño, ya sea de datos personales, financieros, intimidad, correo electrónico y redes sociales.

En relación con los delitos informáticos más frecuentes, el Fiscal indica que la estafa informática, mediante redes sociales, por ejemplo, Facebook, en la más común, tanto con fines de robo de dinero como para seducir a menores de edad.

Cuando se inquiere sobre la dificultad para identificar los sujetos activos, Arias afirma que, efectivamente, es difícil. Por ejemplo, en el caso de defraudaciones, se desvía el dinero y a la persona que se le deposita no es atribuible la responsabilidad penal, porque se actúa con un seudónimo y, para ubicar la dirección IP, los delincuentes saben cómo evadir la investigación.

Arias indica que el mayor problema al enfrentar un proceso judicial de este tipo es el tiempo, pues se debe solicitar levantamiento del secreto bancario, decomisar equipos, analizar la evidencia con el equipo especial del OIJ, entre otras diligencias.

Seguidamente, se cuestiona al entrevistado sobre cuáles son los principales impedimentos u obstáculos para poder procesar penalmente a los delincuentes informáticos. Para él, el principal es identificarlos.

Sobre la consulta de si las universidades deberían incluir los delitos informáticos en la formación, la respuesta es positiva. El entrevistado considera que debe darse una inducción a las nuevas modalidades de delincuencia.

Al solicitar recomendaciones para mejorar los procedimientos en materia penal, señala que, a nivel de Judicatura y circuitos judiciales no existe especialización sobre estos delitos y el Colegio de Abogados o las universidades deberían incentivar los cursos de actualización jurídica sobre esos temas.

Por último, se cuestiona sobre los cambios que la población ha hecho al utilizar Internet. En opinión de Arias, la población “sigue siendo ingenua” (Barrios, 2020); poseer capacidad de engaño, tener debilidad en la seguridad de los sistemas, e incluso, la necesidad financiera son factores que facilitan los delitos.

4.5.2 Fiscal Ovidio González Cruz.

En primera instancia, se consulta qué es un ciberdelito o delito informático. El entrevistado explica que “es aquella acción ilícita que se comete a través de un dispositivo electrónico” (González, 2020).

En relación con el perfil del delincuente, explica, que no existe un perfil o persona determinada, aunque sí se sugiere que lo comete alguien con conocimiento básico en redes y con un ordenador. En algunos delitos no se requiere mayores conocimientos, por ejemplo, en la suplantación, aunque en las grandes estafas se sugiere una mayor preparación.

Cuando se pregunta por los delitos más frecuentes, González indica que es la estafa informática y anota que es “muy difícil determinar quién es el *frentiador*, quién es el que realizó la llamada, el que hizo toda la ingeniería social” (González, 2020).

Al interrogar si es difícil la identificación del actor de esos delitos, el entrevistado afirma que es un poco difícil, pero en casos cuando la dirección IP es estática, puede determinarse de dónde salió la estafa, cuando las ejecutan personas con poco conocimiento, pues hay quienes esconden la dirección IP en diferentes países y logran encriptar ese dato. También, se dificulta cuando la estafa se realiza con el celular, pues este utiliza una dirección IP dinámica y se conecta a varios proveedores.

Se consulta cuál es el mayor problema, judicialmente, al enfrentar un proceso de este tipo de delitos. González indica que la recolección y el tratamiento de la evidencia, así como la falta de capacitación de la Judicatura, pues indica que cuando se realizaba una diligencia “nos rechazaban las solicitudes al no tener conocimiento, nos rechazaban las solicitudes de allanamientos, intervenciones, aperturas o extracción de esa información” (González, 2020).

Ante esa respuesta, se le pregunta al entrevistado si el hecho de que los tipos penales no estén concentrados es un problema, a lo que responde afirmativamente. González considera que debe existir una ley específica que contemple todos los delitos, por lo que debe haber un cuerpo normativo; además, en su criterio es recomendable que no estén repartidos en el Código Penal.

En cuanto a la terminología del tipo penal, el participante explica que se dan confusiones, porque cuando se acude a la autoridad jurisdiccional, si esta no conoce los conceptos, se genera confusión en los operadores del derecho.

Cuando se le pregunta si en las universidades debería prepararse a los estudiantes de derecho en materia de delitos informáticos, responde afirmativamente. Incluso, agrega que tanto en "las universidades como en la unidad de capacitación cuando se prepara a los fiscales" (González, 2020). En la actualidad, agrega, debe ser casi exigida la preparación en este tema.

Al solicitarle recomendaciones, indica que "hay que leer, informarse, consultar" (González, 2020), es importante capacitarse y consultar con otros colegas dentro y fuera del país.

Finalmente, en relación con la tipicidad del tipo penal, artículos 216 o 217 bis, el entrevistado no considera que existan algún problema: el primero se refiere a la estafa común y el segundo, a lo que antes se llamaba fraude informático, en donde ya se utiliza algún medio tecnológico, por lo que, en su criterio, no hay problema.

4.6 Entrevista coordinador Oficina de Investigación sobre delitos informáticos

4.6.1 Máster Roberto Paulo Lemaitre Picado.

Ante la consulta sobre qué es delito informático, Lemaitre explica que es "aquella acción típica antijurídica culpable realizada por medios informáticos para eliminar los datos de un dispositivo informático, tanto en el ámbito jurídico como en lo tecnológico" (Lemaitre, 2020).

Al preguntársele qué ley regula estos delitos, este explica que no hay una ley o código específico, sino que se han hecho reformas al Código Penal. Al respecto, se le cuestiona si debería existir una ley específica, a lo que responde que existen marcos legales, principalmente “el Marco jurídico en materia de tecnologías y delitos informáticos” (Lemaitre, 2020).

Luego, se le inquiere si considera que está bien ordenado el articulado del Código Penal o si debería estar más concentrado. Lemaitre explica que lo importante es contemplarlo y mantener actualizado lo correspondiente tanto en el tema jurídico como en el área tecnológica, se debe hacer un tratamiento interdisciplinario.

En relación con el perfil de quien comete el delito informático, el entrevistado explica que puede realizarlo cualquier persona, desde especialistas en cibercrimen a gente que lo hace por diversión o contratando a alguien. Incluso compartir información sin autorización es violación de comunicaciones, es decir, un delito sin tener preparación alguna.

En cuanto al sujeto pasivo, el entrevistado afirma que quien sufre la afectación, está más expuesto: mujeres, menores de edad, adultos mayores que, por desconocimiento, son susceptibles a engaños.

Se consulta al entrevistado sobre los delitos más frecuentes en el periodo 2019-2020. Este indica que se dieron las estafas informáticas y la suplantación de identidad, delitos que aumentaron con la pandemia y el teletrabajo.

De igual manera, se le pregunta sobre la dificultad para identificar a los sujetos activos, a lo que responde que efectivamente sí es difícil tener acceso a la información. Resalta que, con el Convenio de Budapest, se pretende más colaboración internacional para el acopio de pruebas digitales.

Con referencia a impedimentos y obstáculos, Lemaitre opina que el reto está en tener las pruebas, el entendimiento del delito por parte de jueces, fiscales y abogados, así como comprender cuál figura aplica, cómo y porqué. A esto se suma que la gente conozca los delitos para que denuncie, además de que se requiere más personal y recursos para enfrentar la saturación.

Posteriormente, se solicita su punto de vista sobre si las universidades deberían tener una materia sobre delitos informáticos. El entrevistado emite una respuesta positiva y argumenta que se requiere preparación en el tipo de delito y el medio digital; menciona, además, que ya existen cursos sobre informática social, o bien "digital y tecnologías emergentes" (Lemaitre, 2020) y concluye señalando que espera que exista la maestría en delitos informáticos.

Al solicitarle recomendaciones sobre el procesamiento penal en Costa Rica, el participante establece que se debe actualizar el marco normativo y estar en constante revisión. Recomienda, también, hacer procesos que incluyan tecnología desde el punto de vista del mundo digital. Principalmente, considera que se debe promover que los jueces, fiscales y abogados estén especializados como delitos informáticos.

En la última consulta, se pide la opinión sobre cómo utiliza la población el Internet y señala que, aunque hay más conciencia, falta más "cultura digital para que la gente tome mayores precauciones [para lograr] no solo saber el riesgo sino saber utilizar la tecnología" (Lemaitre, 2020).

4.7 Contraste de las ideas aportadas por los entrevistados

Una vez que se identifican las principales ideas aportadas en las entrevistas, y con el objetivo de evidenciar aspectos relevantes para la investigación, se expone un análisis contrastante de las argumentaciones obtenidas según las categorías de análisis establecidas.

4.7.1 Concepto de ciberdelito o delito informático.

En relación con la definición de delito informático, los abogados defensores concuerdan en que, para considerarlo en esta categoría, en el ilícito debe intervenir el uso de un medio tecnológico; ya sea que se vulnere el sistema o bien, se utilice para cometer el delito. Montero (2020), además, agregó que el bien jurídico son los datos o la información vulnerada.

Para los abogados litigantes, la definición parece no estar tan clara, pues uno de ellos expone la complicación del término y el otro menciona los bienes jurídicos, pero no lo define como tal; sin embargo, resalta el hecho de que incluye como bienes tutelados la confidencialidad y la integridad.

En el caso concreto de los ingenieros en informática, ambos concuerdan en que son acciones ilegales que se utilizan para afectar a terceros.

Por su parte, los jueces consultados concuerdan al definir el término como ilícitos cometidos por medio de la tecnología. Cabe resaltar que, como bienes vulnerados, se exponen el patrimonio, la intimidad, el honor y la reputación.

En cuanto a los fiscales, ambos concuerdan en que se utiliza la tecnología para ocasionar un perjuicio patrimonial; Arias (2020) agrega la moral dentro de los bienes tutelados.

Por último, Lemaitre (2020), concuerda con la mayoría de los entrevistados en cuanto a que se utiliza la tecnología; pero, en su caso argumenta que se utiliza para eliminar datos y ahí es donde se comete la acción antijurídica culpable.

Como se evidencia, todos los entrevistados tienen un común denominador en la definición que dan, pues efectivamente, para cometer un delito de este tipo se requiere de la manipulación de sistemas informáticos y la clara intención de causar daño.

4.7.2 Perfil del delincuente.

Como en todo tipo de delitos es imprescindible conocer el perfil de los delincuentes. Al respecto, los abogados defensores indican que no hay un perfil determinado, aunque sí se argumenta que, al menos, debe tener conocimientos básicos, incluso empíricos, del manejo de sistemas informáticos, pues es importante la manipulación de estos.

En el caso de los litigantes, las respuestas contrastan, pues, mientras Angulo (2020), establece un rango de edad y argumenta que son personas inteligentes y habilidosas, Medrano (2020) argumenta que cualquiera puede ser un ciberdelincuente, desde un especialista hasta un usuario común y corriente.

Ideas similares se encuentran en las respuestas de los ingenieros consultados. Ambos señalan que no hay un perfil específico, pues cualquiera con alguna habilidad en informática o sin ella, puede convertirse en delincuente. Resalta el aporte de Alfaro (2020), quien establece categorías de sombreros: negro, blanco o gris, según su participación.

En el caso concreto de los jueces y los fiscales consultados, concuerdan en que cualquiera puede ser ciberdelincuente, pues solo necesita un medio informático y un conocimiento básico.

Para Lemaitre (2020), ni siquiera se requiere de un conocimiento básico; solo compartir información sin tener permiso de hacerlo, constituye un delito, por lo que cualquiera puede ser ciberdelincuente.

Como se observa, hay un aspecto en común y es el hecho de que para cometer un cibercrimen lo único requerido es la intención de hacerlo, aunque se hace la salvedad que entre más conocimiento tenga ese delincuente, probablemente el daño causado será mayor.

4.7.3 Delitos más comunes en Costa Rica.

Sin duda alguna, es fundamental establecer cuáles son los delitos más recurrentes en la realidad nacional. Al respecto, todos los entrevistados concuerdan en que la estafa o fraude informático es el principal. Barrios (2020) agrega, además, el daño, el sabotaje y la suplantación de identidad. En este tipo de delitos solamente se logra identificar, en algunas ocasiones, a los "frentiadores", es decir, a esas terceras personas a quienes se les vincula con las cuentas donde se deposita el dinero, ya sea porque las prestan o bien porque ignoran que se ha cometido un ilícito.

Este mismo delito es señalado por los ingenieros en informática como el más común, pero agregan otros como la suplantación o la difusión de información; además, señalan un aspecto fundamental y es que, aunque se dan otros ilícitos, estos no son denunciados por las víctimas.

Sobresale el comentario de Lemaitre (2020), al argumentar que este delito de estafa y el de suplantación aumentaron considerablemente en época de pandemia y de teletrabajo. La estafa es, hoy en día, el principal delito informático y, como tal, debe abordarse para tratar de mitigar sus efectos.

4.7.4 Identificación del sujeto activo.

Definitivamente, establecer el perfil de los sujetos activos y pasivos en este tipo de delitos es imprescindible. En el caso del sujeto activo, tanto los defensores y los litigantes como los jueces y fiscales establecen que es muy difícil la identificación, pues el ciberespacio permite a los delincuentes verdaderos ocultarse en la web oscura, desviar las direcciones IP y, por ende, se complica la obtención de elementos probatorios.

En la misma línea de pensamiento se encuentra Lemaitre (2020), quien aporta que convenios internacionales como el de Budapest son imprescindibles para la identificación de los sujetos activos.

Los profesionales en derecho confluyen en la idea de que, al final de los procesos, quien se identifica como sujeto activo es, generalmente, la tercera pieza de la triada, esa persona que saca el dinero o presta su cuenta para cometer el ilícito y que, en algunos casos, no cuenta con conocimiento de causa o bien fue engañada también.

Los ingenieros concuerdan con esas ideas. Agregan que la informática forense es una alternativa, pero se requiere personal calificado para ubicar las huellas digitales.

4.7.5 Identificación del sujeto pasivo.

Desde el punto de vista de los litigantes, jueces y fiscales, el sujeto pasivo puede ser cualquier persona que tuvo acceso a un medio informático y que, ya sea por no tener mucho conocimiento o bien porque fue engañado, facilita sus datos sensibles, claves, correos electrónicos o navega en páginas fraudulentas sin saberlo. Incluso, pueden ser víctimas las entidades bancarias. Resulta importante el aporte de Barrios (2020), quien perfila como víctimas a personas que poseen grandes sumas de dinero o valores. Lemaitre (2020), por su parte, agrega que hay sujetos más propensos a engaños; señala a mujeres, menores de edad y adultos mayores.

Como se aprecia, para ser víctima de estos delincuentes informáticos, solo se requiere una dosis de confianza, desconocimiento y acceso a la informática, desde un medio tan común y generalizado como una red social.

4.7.6 Problemas al afrontar un proceso judicial.

Para los abogados defensores no hay problema como tal, porque las falencias que se encuentran en las investigaciones de este tipo de delitos son más bien un beneficio para sus defendidos. Aun así, señalan que la falta de elementos probatorios y la acreditación de la forma dolosa son aspectos fundamentales para el proceso, que muchas veces termina en sobreseimientos. Además, el anonimato en que trabajan los delincuentes obstaculiza su identificación.

Tanto los litigantes como los jueces y fiscales concuerdan en que entre los problemas están identificar a los autores y que el Organismo de Investigación Judicial no tiene los recursos materiales y humanos para realizar las diligencias necesarias en tiempo y forma, por lo que muchas denuncias se archivan. Con respecto a la identificación de los delincuentes, los ingenieros coinciden, pues no existe el material humano especializado para lograrlo.

Sobresale el aporte de González (2020), al mencionar que falta capacitación en la Judicatura, que por desconocimiento rechazan solicitudes, con lo que se dificulta la recolección y el tratamiento de evidencias.

Además, Lemaitre (2020) aporta otro reto: que los encargados de hacer justicia entiendan los delitos en el cómo y el porqué, aunado a que las personas en general hagan las denuncias correctamente.

4.7.7 Terminología de los delitos informáticos.

Para los abogados en general, tanto litigantes como defensores, la terminología debe corresponder con el área informática. Además, es necesario capacitarse para conocer y dominar el léxico o bien, acudir a consultores técnicos para el mejor abordaje de los casos. Se agrega que, ya que la mayoría de términos son anglicismos, debe considerarse ese aspecto, pues como se indicó en la entrevista del licenciado Angulo Yu, al realizar traducciones al español se puede perder su significado. Incluso sobresale el hecho de que la estafa informática, aunque esté en español, es un término muy amplio, idea que comparten don Henry Angulo y don Joffre Montero, incluso se llega a mencionar que, la existencia per se, de un computador, ya sería delito.

En la opinión de González (2020), el problema radica en que, desde la autoridad jurisdiccional, pueden caer en confusiones los operadores del derecho, por desconocimiento de los términos. Esto deriva en procesos penales que no llegan a concluirse satisfactoriamente o incluso

en investigaciones que se extienden mucho por la necesidad de intervención de peritos para aclarar términos propios del área tecnológica.

Con lo anterior, se evidencia que, si se trata de delitos informáticos, se requiere conocer o bien, acudir a quien conoce del área, para poder hacer un abordaje adecuado. Como se evidenció, la presencia de un perito o experto en el área informática es fundamental para esclarecer conceptos y poder aplicarlos desde la óptica del derecho.

La terminología debe ser sumamente clara y no ocasionar ningún tipo de confusión en los actores de derecho, ya sea acudiendo a peritos o expertos, lo importante es establecer, correctamente, la figura delictiva, desde que se formula la denuncia hasta su resolución final.

4.7.8 Preparación desde las universidades en materia de delitos informáticos.

Ante el auge que parece tener el cibercrimen donde, cada minuto, surgen nuevos virus o intentos de estafa digital y delitos encubiertos en la *web*, como se ha puntualizado, parece fundamental que los operadores del derecho conozcan conceptos básicos suficientes en el área de informática y del cibercrimen. Al respecto, los defensores públicos, concuerdan en que se debe trabajar desde las universidades para prepararse, desde la licenciatura o el posgrado, pero debe existir también motivación y dedicación para capacitarse.

En lo que respecta a los fiscales, se obtuvieron dos posiciones contrastantes; mientras uno indica que la materia de delitos informáticos en universidades debe ser optativa, su colega enfatiza que debe darse Derecho Informático, al ser delitos que se acrecientan constantemente.

Esta última idea es compartida por los ingenieros, quienes expresan la necesidad de preparar no solo a los abogados, sino a todo el personal forense e investigador.

Los jueces entrevistados lo consideran imprescindible. Además de la necesidad de impartir esa materia en las universidades, agregan que debe enseñarse el análisis del tipo penal, para

solventar el problema de pruebas en los procesos. Esta idea es compartida por Lemaitre (2020), quien además opina que debería existir la maestría en delitos informáticos.

Sin lugar a duda, los centros universitarios son clave en la preparación de operadores del derecho para el tratamiento del cibercrimen.

4.7.9 Recomendaciones para los procesos en materia de delitos informáticos.

Para los abogados defensores, se requieren alianzas entre el OIJ y las entidades bancarias, además de la capacitación y especialización de los involucrados en los procesos. Todo esto con el objetivo de realizar acciones inmediatas, pues en estos delitos el tiempo es fundamental.

Los litigantes concuerdan en el tema de la capacitación y agregan mejoras en el recurso humano y material, de generar una cultura criminal y de dotar de presupuesto suficiente a las instituciones de investigación.

Para los jueces, la clave para mejorar está en la efectividad del Ministerio Público, al solicitar, por ejemplo, levantamiento de secreto bancario y recopilar y aportar pruebas. Solamente Barrios (2020), propuso un cambio en la ley; para él, se necesita agilizar el marco de acción de la fiscalía y el OIJ para evitar la impunidad.

Los fiscales agregan que se requieren especializaciones en la Judicatura y Circuitos Judiciales, además de capacitación y consulta dentro y fuera del país.

Por último, Lemaitre (2020) recomienda actualizar el marco normativo y concuerda con otros entrevistados en que los operadores del derecho deben especializarse en el tema de delitos informáticos.

4.7.10 Tipicidad de los delitos informáticos.

Como se analizó en el desarrollo del trabajo la tipicidad es fundamental para el abordaje de los delitos informáticos, pues permite determinar si la conducta perpetrada se adecúa a la ley penal, pues si existe una conducta atípica se vuelve relevante para el derecho penal.

Desde la óptica de los defensores públicos, el problema de la tipicidad está en la amplitud; con términos poco claros, se presentan interpretaciones diferentes, en el caso específico de la estafa informática, la ley indica que se debe considerar si se vulnera un sistema informático y al no existir tal daño al *software*, se encasilla el fraude como tradicional y típico y no como un ciber crimen, más bien como un caso de estafa común.

En la tipificación de los delitos existe falta claridad. Desde el conocimiento del ciudadano común, para acudir a imponer la denuncia, hasta los garantes de la ley y su aplicación en instancias judiciales.

En contraposición, los fiscales indican que los artículos 216 y 217 Bis del Código Penal son claros. El primero se refiere específicamente a la estafa común, mientras que el 217 bis es específico del delito informático.

4.7.11 Seguridad sobre los delitos informáticos.

A este respecto, los abogados litigantes concuerdan en que debe evitarse suministrar datos sensibles y tratar de educarse en seguridad a la hora de utilizar redes sociales, por ejemplo.

La opinión de los jueces es dicotómica. Ramírez (2020), considera que la población, es más precavida ahora; por su parte, Barrios (2020) expresa que la gente sigue facilitando claves y cuentas. Sin embargo, ambos concuerdan en que hay quienes siguen cayendo en engaños.

Desde la óptica fiscal, Arias (2020) considera que existe todavía mucha ingenuidad; prevalece la capacidad de engaño, quizás motivada por la necesidad de las personas o la

vulnerabilidad de los sistemas informáticos. La apreciación de Lemaitre (2020) concuerda con el fiscal, pues indica que falta mucha cultura digital para evitar el delito y saber utilizar la tecnología.

4.8 Análisis de la jurisprudencia en materia de delitos informáticos

4.8.1 Resolución N. 00494 – 2020. II Circuito Judicial de San José.

Fecha de la Resolución: 26 de marzo del 2020
Expediente: 16-003520-0059-PE
Temas (descriptores): estafa informática
Subtemas (restrictores): confirmación de absolutoria en caso de imputados acusados de prestar sus cuentas bancarias para recibir dineros de forma ilícita
Tipo de contenido: voto de mayoría
Rama del derecho: Derecho Penal

En primera instancia, se explica que este caso en particular analiza una acusación por el supuesto préstamo de las cuentas bancarias del imputado, para recibir dineros producto de una estafa informática, en perjuicio de un tercero. A la víctima le realizó una llamada un supuesto funcionario bancario y se le solicitó información sensible, cuentas y claves de acceso, para realizar el fraude. Posteriormente, se trasladó el dinero entre cuentas para cometer el delito.

En sentencia N.º 1130-2019, dictada por el Tribunal Penal del Primer Circuito Judicial de San José, el 01 de octubre de 2019, se absolvió a los encartados del delito de estafa informática, por lo que el Ministerio Público, presenta la apelación correspondiente.

La fiscalía argumenta, en primer lugar, que el acusado se presentó a la entidad bancaria a retirar el dinero instantes previos al depósito realizado mediante el delito de estafa. En segundo lugar, se alega inobservancia al no considerarse la aplicación del artículo 217 bis del Código Penal, puesto que los acusados, si bien no realizan la llamada ni transfieren el dinero, son coautores del delito al prestar sus cuentas bancarias para el depósito del bien sustraído, lo que supone un acuerdo previo para la comisión del dolo.

En un tercer lugar, se argumenta “errónea valoración de la prueba testimonial”; la testigo explica que, cuando se percató de la situación, consultó a la dueña de la cuenta donde provenían los montos y esta expresó que no había realizado transacción alguna. A lo anterior se suma que la cuenta para cometer el ilícito era de reciente apertura.

La cuarta razón expuesta fue “la inobservancia del deber fundamentación, sobre la valoración de la prueba bancaria”, pues para considerar a los acusados culpables, se asumió que debían tener antecedentes judiciales en hechos similares y no se analizó adecuadamente la información proveniente del levantamiento del secreto bancario, en relación con movimientos de las cuentas involucradas.

La defensa refuta los motivos y argumenta que no se comprueba si su representado actuó con conocimiento y voluntad en la estafa ni la procedencia del dinero producto de una acción ilícita. Alega, además, que no hay elemento probatorio de la coautoría o acuerdo previo para realizar el delito; agrega que la estafa informática es un tipo penal que solo admite dolo directo. Con respecto al tercer motivo, alega la defensora que la testigo no puede demostrar que su representado hiciera la llamada o la transferencia denunciadas. Por último, tras el alegato de la fiscalía de que los acusados formaban parte de una organización criminal, no hubo respaldo probatorio en sus expedientes judiciales.

El alegato de la fiscalía es rechazado. En este caso en particular, se salva el voto de una de las jueces y los otros dos explican sus razones.

En primera instancia, explica el juez, porque se lleva a cabo la estafa mediante una llamada, en la que, por conferencia telefónica, un sujeto se hace pasar por comprador de bienes pertenecientes a la víctima y otro actúa como funcionario del banco y extraen la información de las cuentas y claves, para realizar las transferencias de distintas cantidades de dinero, en colones y

dólares, a las cuentas de terceros. Al percatarse del fraude, la entidad bancaria reporta y son detenidos los imputados. Sin embargo, no se comprueba "el elemento subjetivo doloso (conocimiento y voluntad) de los acusados para la comisión del tipo penal de la estafa informática".

Explica el juez prestar las cuentas a terceros puede contravenir las normas del banco y ocasionar un posible cierre de estas, pero no una sanción penal. En cuanto a lo obtenido tras el levantamiento del secreto bancario, solo se evidencian las transferencias, pero no que los acusados conocían de alguna acción fraudulenta detrás de dichas transacciones.

Se aplica, en este caso, el principio de duda razonable, ya que, "de conformidad con el artículo 45 del Código Penal, son coautores quienes realicen el hecho punible tipificado juntamente con el autor" y no existe prueba idónea, para relacionar a los acusados con el sujeto activo del delito de estafa informática, ni con los otros *frentiadores*.

Por su parte, la segunda jueza expone que "la acusación formulada por el órgano requirente no contiene los elementos necesarios para atribuir a estos una coautoría en el delito de estafa informática". Sus argumentos son similares a los del juez anterior; sin embargo, la jueza agrega que no se logra probar, por parte de la fiscalía, que los acusados "actuasen de común acuerdo con quien, usando indebidamente los datos que obtuvo vía telefónica de la víctima, manipuló el ingreso y procesamiento de esos datos en el sistema informático del Banco Nacional de Costa Rica y trasladó dinero de la cuenta". Aporta, como dato importante, que se desconoce quién es realmente el sujeto activo del delito de estafa informática.

La tercera jueza salva el voto, argumentando razones de orden jurídico. Los acusados fueron contactados por un desconocido y le facilitaron sus cuentas bancarias para realizar transferencias el mismo día que se realiza la estafa telefónica y se transfieren los fondos; uno de

los acusados logra retirar el dinero y a otros se les detectó a tiempo: se bloquearon las cuentas y fueron detenidos, antes de concretar el retiro.

La jueza argumenta que debió darse un análisis más profundo, por tratarse de un delito de estafa informática y que "debe considerarse que este tipo de delincuencia a ser novedosa en nuestro sistema de justicia penal requiere que las personas juzgadoras realicen un análisis comprensivo, amplio y bien ponderado de todas las actuaciones realizadas por el autor o autores". Además, agrega que, si bien los acusados no realizan la llamada ni las trasferencias de dinero, se debió analizar su participación para determinar si se dio un dolo directo, si conocían el origen fraudulento del dinero o tenían justificación para que se transfirieran altas sumas de dinero a sus cuentas.

En su argumentación indica, además, que no tener en el expediente judicial hechos similares a los denunciados, no niega la posibilidad de cometerlos. Concluye su explicación justificando la nulidad de su voto pues existió "un déficit en el análisis de la tipicidad de la conducta acusada".

4.8.2 Resolución N. 01076 - 2020. Sala Tercera de la Corte.

Fecha de la Resolución: 28 de agosto del 2020
Expediente: 13-001603-0042-PE
Temas (descriptores): estafa informática
Subtemas (restrictores): bien jurídico tutelado
Tipo de contenido: voto de mayoría
Rama del derecho: Derecho Penal

Para interés del análisis de jurisprudencia, se explica en el texto de la resolución que la falta se les imputa a cinco acusados por estafa informática en prejuicio del Banco de Costa Rica y otros. El delito se comete en tanto se utilizan tarjetas falsas de débito y crédito, clonadas y que pertenecen a otros sujetos, para dispensar dinero de varios cajeros automáticos, en fechas y lugares diferentes.

Para la comisión de la estafa, los acusados planificaron obtener beneficios económicos antijurídicos. Para ello, se apoderaron de tarjetas falsificadas de crédito y débito para utilizarlas en compras y retiros de dinero en diversos comercios del país. Se apropian de la información contenida en las bandas magnéticas de las tarjetas y realizan la clonación, sin que exista claridad en cómo lo hacen, para luego hacer efectivo el uso y la estafa a los verdaderos tarjetahabientes.

Se considera estafa, pues, a la "manipulación del sistema informático para obtener un beneficio patrimonial antijurídico", al utilizar el cajero automático, dar órdenes para dispensar tractos de dinero específicos y a la tarjeta de crédito copiada, para intentar pagar por bienes mediante transacciones que resultaron denegadas, con una clara finalidad delictiva de lesionar el patrimonio ajeno.

Se presentan recursos de apelación por parte de los imputados y se recalifican los delitos como estafa informática en conformidad con las reglas del delito continuado, se mantienen las medidas cautelares.

Por parte del Ministerio Público, se presenta recurso de casación en contra de la resolución número 2019-1945, del 30 de octubre de 2019, dictada por el Tribunal de Apelación de la Sentencia Penal del Segundo Circuito Judicial de San José, Goicoechea. Se "alega la inobservancia del artículo 76 del Código Penal y la errónea aplicación del numeral 75 del mismo cuerpo legal". Se argumenta, además, que las transacciones hechas fueron cometidas en concurso material, puesto que, aunque hay diferencias temporales en la comisión del delito, en todas "se requirió de la manipulación, el influjo o el mal uso de los datos para procurar el beneficio patrimonial antijurídico, por lo que se consumó el delito de forma homogénea configurándose dos delitos de estafa informática en concurso material"; razón por la cual, se solicita la aplicación reglas del delito continuado.

Como se evidencia, existe un debate por el hecho de que las transacciones se consideran un solo delito y no delitos independientes. El Ministerio Público alega que, aunque se vulneró el mismo sistema informático del mismo bien jurídico y al mismo sujeto pasivo, se dieron varias acciones; el sujeto activo, consciente de la falsedad de la tarjeta, incurrió en varias acciones delictivas.

La fiscalía alega que los acusados realizaron retiros y compras con las tarjetas clonadas y, por tanto, se cometen varias estafas, pues "cada delito se configuró desde el momento en que el agente activo, a sabiendas de la falsedad de la tarjeta, realizó cada una de las transacciones o cada uno de los retiros de los cajeros".

Para el representante del Ministerio Público, es un error "calificar los hechos acusados y acreditados como constitutivos de los delitos de estafa informática en concurso material, en la modalidad de delito continuado, pues dicha fijación se realizó en estricto apego a los artículos 76 y 77 del Código Penal". Agrega que los hechos acreditados se dieron de forma independiente.

Sin embargo, pese a los argumentos presentados, la Sala consideró que se cometió una única acción delictiva y se fundamentan en el tipo penal de estafa informática que está regulado en el artículo 217 bis del Código Penal, pues se dio la manipulación del sistema informático, donde el cajero puede obtener un beneficio patrimonial antijurídico; además, los imputados utilizan datos falsos, entiéndase las tarjetas clonadas, para realizar compras. Para la consideración de la Sala, se comete un solo acto con la misma finalidad.

Se establece, entonces, que "el sujeto pasivo es el mismo, como también lo es el bien jurídico tutelado que resulta lesionado, lo que implica una sola acción en sentido jurídico penal y evidencian una sola resolución criminal" (Resolución N.º 01076 – 2020), razón por la cual se dejó sin lugar el recurso de casación.

4.9 Contraste de ideas emitidas en las entrevistas y la jurisprudencia analizada

Luego del análisis de las resoluciones, tanto de la Sala Tercera como del II Circuito, se encuentran coincidencias entre el tratamiento del delito, principalmente de estafa informática, y los aportes que facilitaron los entrevistados, operadores del derecho.

Con base en la jurisprudencia encontrada y analizada, en Costa Rica, el delito informático más recurrente es el de estafa informática, principalmente por fraude con tarjeta de crédito o débito o mediante el timo o engaño telefónico, en el que se extraen datos sensibles como cuentas bancarias o claves de acceso. Para ello, los ciberdelincuentes se valen de timos para engañar a los sujetos pasivos.

Los operadores del derecho externaron, en sus propuestas argumentativas, que determinar el sujeto activo, en este tipo de actividad delictiva, es muy difícil, casi imposible. Como se evidencia la Resolución N.º 00494 – 2020, en la estafa realizada, identificar a quién realiza la llamada y quién ejecuta las transacciones entre cuentas es imposible para la fiscalía; únicamente se logra determinar quiénes son los dueños de las cuentas facilitadas al desconocido.

Como han señalado los entrevistados en sus argumentos, el sujeto pasivo puede ser cualquier persona, solo se requiere un engaño, exceso de confianza o un trabajo bien elaborado, como ocurre con las tarjetas clonadas, evidenciado en la Resolución N.º 01076 – 2020. Desde un individuo hasta una entidad bancaria pueden ser vulnerables a delitos informáticos.

No se logra demostrar que los acusados, en la Resolución N.º 00494 – 2020, actuaron con dolo. No existen elementos probatorios y se trata de *frentiadores*, cuya participación intencional y criminal en el delito no se logra comprobar, pese a las características de los retiros y movimientos que realizan.

Es importante rescatar el argumento realizado por una de las juezas de esta sentencia, quien aduce que los acusados actúan incorrectamente al facilitarle a un desconocido sus cuentas bancarias para realizar transferencias de grandes cantidades de dinero, del cual, supuestamente, desconocía el origen. Sin embargo, lo mencionado por la jueza no se encuentra tipificado como delito penal.

La falta de tipicidad es otro de los aspectos que se desprende tanto de las entrevistas como de las resoluciones estudiadas. Al aplicar el artículo 217 bis, los operadores del derecho realizan interpretaciones varias, por lo que falta claridad o, más bien, hay mucha amplitud en el término. Sin lugar a duda, y en concordancia con la posición de Lemaitre (2020), se requiere especialización en este tipo de delitos y su abordaje.

Los datos aportados por el análisis, tanto de las entrevistas como de la jurisprudencia, permiten comprobar que hay una incidencia directa en los elementos normativos de los tipos penales, especialmente, el de la estafa informática, pues la interpretación que se hace del artículo 217 bis condiciona el resultado de la sentencia, la defensa misma o la posición del Ministerio Público. Como se evidencia, puede considerarse un delito prestar las cuentas personales para el fraude, pero sin los elementos probatorios de que ese *frentiador* actuó con dolo, es imposible comprobar su coautoría en los hechos.

Con respecto a los delitos de suplantación y difusión de información falsa, no se encontró jurisprudencia en el periodo 2019-2020, en la Sala Tercera y el II Circuito Judicial de San José. Esto puede deberse a factores como que las víctimas no llegan a realizar las denuncias por desconocer que es un delito como tal o, cuando se apersona a la autoridad correspondiente para denunciar, el personal de justicia desconoce cómo debe tipificarse la falta cometida, lo que deriva en que la denuncia no trascienda como debe o sea archivada.

De acuerdo con los datos analizados, la configuración típica de estos dos delitos debe modificarse o deben realizarse mayores y mejores esfuerzos por informar y que las víctimas entiendan cómo denunciar.

Por otro lado, se quiere hacer resaltar cual es la importancia de la jurisprudencia seleccionada, y para ello es necesario analizar que, en un alto número de sentencias por Estafa informática, no existe manipulación de sistemas informáticos por parte de los procesados, sino más bien se hace referencia a la utilización de tarjetas de pago, sean porque las mismas fueron clonadas, o porque los indilgados prestaron sus cuentas bancarias para que se les depositara el dinero proveniente del ilícito. Se realiza la acción investigada en el ámbito físico, se da una comunicación entre personas, por lo que no deberían ser procesados a través de la figura de Estafa informática, lo cual trae consigo una violación al principio de legalidad.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Una vez finalizada esta investigación y con referencia en los objetivos planteados sobre el tema de la especificidad de la configuración típica de los delitos informáticos y su incidencia en los procesos penales, especialmente, la configuración típica de los elementos normativos de los tipos penales informáticos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236) todos del Código Penal costarricense y su incidencia en los resultados de los procesos penales, se tienen las siguientes conclusiones:

1) Con los avances vertiginosos de la tecnología y las comunicaciones, el cibercrimen se expande y modifica constantemente y les permite a los delincuentes diversificar sus acciones en perjuicio de víctimas, que, por su confianza o falta de conocimiento, se vuelven presa fácil de delitos informáticos.

2) Tanto el Ministerio Público, como el Organismo de Investigación Judicial y las entidades bancarias carecen de la capacidad para detectar las acciones ilícitas fraudulentas y para identificar a los culpables; tan solo se logra revelar el fraude cuando la víctima observa movimientos sospechosos en su cuenta bancaria. Por lo que identificar al sujeto activo y recuperar el dinero sustraído es casi imposible.

3) Entre los principales problemas que existen al enfrentar los delitos informáticos están, en primer lugar, el factor tiempo: se debe solicitar levantamiento del secreto bancario, decomisar equipos, analizar la evidencia con el equipo especial del OIJ, entre otras diligencias; en ese lapso, los ciberdelincuentes podrían ocultar su huella. En segundo lugar, el uso de una VPN y el tránsito en la *web* oscura, pues los sujetos delictivos se vuelven casi anónimos mediante la manipulación de las direcciones IP y borran todos

los rastros. Por último, la dinámica compleja de los delitos y la internacionalización, al existir la globalidad de los datos, pues un ciberdelincuente podría estar en cualquier parte del mundo.

4) La terminología de los tipos penales informáticos es técnica y compleja. En ocasiones, la autoridad jurisdiccional no conoce los conceptos y esto crea gran confusión en los operadores del derecho. En el caso de la estafa informática, contiene variedad de verbos, que vuelve muy amplio. En cuanto a la suplantación de identidad y la difusión de información falsa, las víctimas prefieren reportar el perfil falso en la red social que denunciarlo; y los casos denunciados en su mayoría son sobreseídos en virtud que es difícil ubicar al sujeto activo o bien, al denunciarlos no se tipificó adecuadamente.

5) Sobre el planteamiento del problema de este estudio, en cuanto a la incidencia o repercusión de la configuración típica de los elementos normativos de los tipos penales informáticos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236) en los resultados de los procesos penales y tomando como referente las resoluciones de la Sala Tercera y los Tribunales de Apelación de Sentencia Penal del año 2019 y 2020, se logra comprobar que existe una incidencia directa de la configuración típica de los delitos informáticos, en virtud de los tecnicismos que conllevan y el lenguaje utilizado. Este supone una preparación en el área informática para su correcta comprensión, lo que deriva en la aplicación más eficiente y eficaz de la ley con relación a casos de cibercrímenes.

6) El problema sobre ciberdelincuencia no ha sido entendido ni abordado de manera correcta en Costa Rica. A la fecha, los delitos informáticos no se encuentran unificados,

tampoco se evidencia una terminología definida, su comprensión es compleja y, al aplicarla, se presentan ambigüedades y vacíos de interpretación.

7) Como resultado de la indagatoria a los actores del derecho y especialistas, se puede concluir que sí existe incidencia en las acciones penales de los delitos informáticos estudiados, puesto que el conocimiento, la valoración de la falta y el tipo penal, son clave para el juzgamiento, principalmente por tres razones: En primer lugar, la amplitud de los artículos, en especial del 217 bis, genera ambigüedad e interpretaciones diversas que recaen directamente en los resultados y tratamiento de las resoluciones penales. En segundo lugar, con base en el aporte argumental de los profesionales consultados, se evidencia que, en la mayoría de casos, el delito de estafa informática es asumida desde la óptica de la estafa común, lo que desvirtúa la aplicabilidad legal. La tercera razón evidenciada es que, la difusión de información falsa y la suplantación de identidad, ni siquiera llegan a instancias judiciales, por falta de denuncias o bien, porque se tipificas erróneamente, desde un primer momento de proceso.

8) Dentro de las limitaciones de la propuesta investigativa, se encuentra el hecho de que no existe, en la Sala Tercera y II Circuito Judicial de San José, jurisprudencia de los delitos de suplantación de identidad y difusión de información falsa, al menos en el lapso tomado en cuenta en esta investigación. Lo que evidencia la falta de denuncias o problemas en el tratamiento del delito al tipificarlo como tal.

9) Se trabaja con jurisprudencia únicamente del año 2020 al no tramitarse resoluciones sobre delitos informáticos en el año 2019 en las dependencias judiciales seleccionadas para la propuesta investigativa.

5.2 Recomendaciones

Con el objetivo de buscar alternativas de mejora ante la problemática analizada, se formulan las siguientes recomendaciones:

1) Mejorar la forma como están escritos los delitos informáticos. La ley penal debe ser más clara para que la persona común pueda entenderla, lo cual resulta lógico si se analiza que los delitos informáticos pueden darse en cualquier estrato social o situación, máxime con el creciente auge de los medios tecnológicos y la comunicación global.

2) Actualizar el marco normativo y crear una ley penal especial solamente para delitos informáticos, con un glosario de definiciones de los conceptos de los tipos penales específicos, que sea comprensible para todos los operadores de la ley y que pueda comunicarse a la población en general; esto último con el fin de que se interpongan denuncias correctamente cuando son víctimas de estos delitos.

3) Realizar una revisión detallada del artículo 217 bis del Código Penal, en virtud que cuanta con muchos verbos típicos, además que parece ser un tipo penal abierto, lo cual se debe modificar.

Recomendación de los entrevistados

1) Capacitar a los funcionarios operadores del derecho y a la policía judicial en la investigación de los delitos informáticos, así como, a los ingenieros informáticos que trabajan para el Poder Judicial, con el objetivo de que estén actualizados y puedan coadyuvar en la lucha contra el flagelo de los delitos informáticos. De imperiosa

necesidad, se debe capacitar a los profesionales como abogados litigantes por parte del Colegio de Abogados relacionado a esta temática.

CAPÍTULO VI: PROPUESTA

Gracias a la investigación realizada, se logra determinar que la terminología de los tipos penales informáticos es técnica y compleja, por lo que los conceptos crean gran confusión en los operadores del derecho. En relación a con la forma en que están construidos los tipos penales informáticos, en este trabajo se ha investigado desde el objetivo general: Analizar si la especificidad de la configuración típica de los elementos normativos de los tipos penales informáticos de estafa informática (artículo 217 bis), suplantación de identidad (numeral 230) y difusión de información falsa (artículo 236), todos del Código Penal costarricense, repercute en los resultados de los procesos penales. En cuanto a las entrevistas realizadas en este trabajo, los entrevistados han sido claros al manifestar que la terminología informática crea confusiones en los operadores del derecho; de igual forma la bibliografía consultada.

En aras de solventar el problema de la configuración típica de los delitos investigados, se propone implementar una ley penal especial sobre delitos informáticos. Esta debe contar con las definiciones de los términos informáticos, con el fin de que toda la población costarricense pueda tener acceso y comprensión de lo que tipifica la legislación. Asimismo, esta debe encontrarse en un solo cuerpo normativo, lo que facilitaría su lectura e interpretación; además, debe cumplir con el derecho constitucional de derecho a la justicia.

En consecuencia, se propone que se implemente un proyecto de ley en el cual se agrupen los delitos informáticos, los cuales son una serie de conductas que están ocasionando un grave daño a los habitantes costarricenses en su patrimonio y su integridad moral, por lo que se requiere que la norma sea clara en las acciones que tipifica. Los costarricenses, al utilizar las plataformas tecnológicas, se ven expuestos a la ciberdelincuencia. Las investigaciones más recientes del

Organismo de Investigación Judicial reflejan que dicha delincuencia tiene una tendencia al aumento, con el agravante de que los medios tecnológicos tienen un crecimiento acelerado. Se debe entender por delitos informáticos la forma en que la población costarricense sufre la intromisión de la delincuencia informática actualmente. El actuar delictivo socaba el patrimonio de las personas, de manera tal que surge inseguridad en la población al crear noticias falsas, por lo que se está llegando al punto en que ya no se sabe qué es verdad en las redes; ahora se habla de posverdad, que trae consigo una sensación de inseguridad generalizada. De igual forma, con la suplantación de identidad, las personas experimentan zozobra y confusión. De ahí la importancia que tiene, para Costa Rica, que los tipos penales de delitos informáticos, sean de lectura comprensible; ya que, la forma en la que están escritos, en la actualidad, únicamente, pueden ser entendidos en su totalidad por una persona con suficientes conocimientos en el área de informática.

Por consiguiente, se deben poner en marcha medidas concretas, pues es el momento preciso para realizar un esfuerzo de agrupar el ordenamiento jurídico que regula los delitos informáticos. La forma de hacerlo es a través de la creación de una ley especial separada del Código Penal, con las definiciones de los verbos típicos que, además, deben resultar comprensibles para quien los lea, de manera que la tramitación a nivel judicial sea fluida y no dé espacios a confusiones en cuanto a la interpretación de los tipos penales informáticos, con el beneficio que sea de fácil de comprender para la población costarricense.

Además, los delitos informáticos que están en el Código Penal se deben extraer de dicho cuerpo normativo y adjuntar a la ley especial, de tal forma que estén unificados y comprensibles, tanto para los operadores del sistema judicial como para la población en general. Lo anterior facilitaría a la población costarricense el tener impresos los delitos informáticos en un solo cuerpo normativo y que estos estén unificados, lo que, evidentemente, implica que estén ordenados y, al

contar con las definiciones de los anglicismos informáticos, dará lugar a una interpretación más correcta de lo que el término informático significa. Los verbos de los delitos informáticos tienden a ser confusos y complejos; palabras como procesamiento, sistema automatizado, programación, operación informática y artificio tecnológico, son sumamente técnicos y de difícil comprensión. Hay que destacar que, en el artículo 217 bis del Código Penal, queda un vacío cuando se lee lo siguiente: "o bien, por cualquier otra acción", lo cual crea la sensación de que el legislador quiso abarcar mucho y, por su amplitud, es uno de los términos más oscuros en dicha norma y da la impresión de ser un tipo penal abierto. Por este motivo, se deberá realizar una revisión de los delitos informáticos existentes, con el fin de poder realizarles las correcciones necesarias, además de implementar nuevos tipos penales, entre los que destaca por su ausencia el delito contra el honor en las redes sociales.

Todos los argumentos previos sustentan la propuesta de la creación de una ley sobre delitos informáticos separada, la cual integre, en un solo cuerpo normativo, los artículos del Código Penal vigente, sobre la citada delincuencia. Esta ley específica requiere de definiciones de los términos de delitos informáticos, cada uno de verbos que contempla el tipo penal de delito informático; debe ser claro, en la actualidad las construcciones literales en los tipos penales informáticos crean muchas dudas en cuanto a la interpretación. Si bien es cierto en Costa Rica se han hecho esfuerzos por tipificar este tipo de conductas, y las autoridades son conscientes de la problemática que ha venido intrínseca con las nuevas tecnologías, el país como tal no debe enfrascarse en la creación de tipos penales confusos, de difícil interpretación, aunque se reconoce el esfuerzo en la creación de tipos penales con el fin de proteger a la población de esta novedosa forma de delinquir, se deben crear tipos penales que resulten claros y comprensivos, ya que de ahí surgirá su efectividad en los procesos que se investiguen a futuro.

REFERENCIAS BIBLIOGRÁFICAS

ACENS Technologies. (s.f.). Recuperado de https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf

Acurio Del Pino, S. (2010). *Delitos Informáticos: generalidades.* Organización de los Estados Americanos. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Albizuri, B. (2002). El Fraude y la Delincuencia Informática: Un Problema Jurídico y Ético. *Revista digital universitaria. Instituto Tecnológico Autónomo, 3*(2). Recuperado de http://www.revista.unam.mx/index30jun2002.html

Alfons, R. (2000) Ventajas Competitivas a través de Sistemas de Información: Más que un Lujo, una Necesidad. México: Mc Graw Hill.

Amorós, M. (2018). *Fake.News: La verdad de las noticias falsas.* Barcelona: Plataforma Editorial.

Área Tecnología. (s.f.). *Recursos, Conocimientos y Temas de Tecnología*. Recuperado de https://www.areatecnologia.com/informatica/tipos-de-malware.html

Arreola, J. (2017). *Delito de usurpación de identidad. La homogenización del Sistema Jurídico.* México: Flores Editor y Distribuidor.

Asamblea Legislativa. (2012). *Expediente N.º 18.546.* Comisión Permanente Especial de Derechos Humanos, Departamento de Comisiones, San José. Recuperado de http://proyectos.conare.ac.cr/asamblea/18546%20dic.pdf

Ávila, W. D. (2013). Hacia una reflexión histórica de las TIC. *Hallazgos, 10*(19), 213-233. Recuperado de https://www.redalyc.org/pdf/4138/413835217013.pdf

Bacigalupo, E. (1996). *Manual del Derecho Penal.* Colombia: Temis.

Barrantes, J. (2020). *Suplantación de identidad en Costa Rica*. ABC Consulting CR. Abogado Penalista. Recuperado de https://www.abcconsulting-cr.com/suplantacion-de-identidad-en-costa-rica/

Bonilla, E., & Rodríguez, P. (1997). *Más allá del dilema de los métodos. La investigación en ciencias sociales.* (3ª Ed.). Santa Fe de Bogotá: Ediciones Unidades.

Bonilla, P. (2019). El espectro actual de los delitos informáticos. *Revista Judicial de Costa Rica* (126), 220-225.

Castillo, F. (2020). Delitos informáticos de Lege y Lege Ferenda. *4to Círculo Pedagógico: Delitos informáticos de Lege Lata y Lege Ferenda*, (pág. Modalidad Virtual).

Ciro, L. A. (2009). *El léxico de la informática y la Internet en algunos países de habla hispana. Hacia una propuesta descriptiva y contrastiva.* Tesis para optar por el título de Doctorado, Universidad de Lleida, España.

Comisión Presidencial coordinadora de la Política del Ejecutivo en materia de Derechos Humanos (COPREDEH). (2011). *DECLARACIÓN UNIVERSAL. Versión comentada.* Ciudad de Guatemala, Guatemala: Autor. Recuperado de https://www.corteidh.or.cr/tablas/28141.pdf

ContenLab. (7 de junio de 2019). Fake News: ¿Cuánto nos afectan las noticias falsas? *El Comercio*. Recuperado de https://elcomercio.pe/especial/perusostenible/paz/fake-news-cuanto-nosafectan-noticias-falsas-noticia-1994336

Coral, A. M. (2012). Una propuesta de análisis jurisprudencial desde el discurso para casos de violencia contra las mujeres en el marco de violencia de pareja. *Opinión Jurídica 11*(22), 17-30.

De la Mata Barranco, N. (2007). *Los delitos cometidos a través de sistemas informáticos.* Bilbao, España: Publicaciones de la Universidad de Deusto.

De las Heras, L. (19 de mayo de 2020). *Las fake news ante el derecho penal español*. Instituto de Derecho Iberoamericano. Recuperado de https://idibe.org/tribuna/las-fake-news-ante-derecho-penal-espanol/

DPEJ.RAE. (2020). *Diccionario panhispánico del español jurídico.* España: Autor. Recuperado de https://dpej.rae.es/lema/suplantar

Estudio de Comunicación. (2018). *Influencia de las noticias falsas en la opinión pública*. España: Servimedia. Recuperado de https://www.servimedia.es/sites/default/files/documentos/informe_sobre_fake_news.pdf

Fábregas, L. (1991), Sistemas de Información, Planificación, Análisis y Diseño. Caracas: Miro.

Faraldo, P. (2010). Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico. *Revista de Derecho Penal y Criminología, 3a. Época,* (3), 73-134. Recuperado de http://e-spacio.uned.es/fez/eserv/bibliuned:revistaDerechoPenalyCriminologia-2010-3-5030/Documento.pdf

Faraldo, P. (2007). *Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática.* España: Eguzkilore.

Fernández, V. (2020). *Consulta Estadística de Delitos Informáticos Periodo del 08/08/2018 al 22/10/2020. ID-46848.* San José, Costa Rica: Organismo de Investigación Judicial, Unidad de Análisis Criminal.

Gascón, D. (18 de junio de 2018). *10 apuntes sobre la posverdad. Notas sobre noticias falsas, propaganda política y 'la verdad de las mentiras'*. Recuperado de https://www.letraslibres.com/espana-mexico/politica/10-apuntes-sobre-la-posverdad

Gómez, B. (2017). *Derecho a la identidad y filiación.* Madrid, España: Dykinson.

González, J. (2008). *Teoría del Delito. Programa de formación inicial de la Defensa Pública.* Costa Rica: Poder Judicial.

González, S. (2020). *"FAKE NEWS" Y RESPONSABILIDAD PENAL*. Bufete Barrilero y Asociados. Recuperado de https://www.barrilero.com/fake-news-responsabilidad-penal/

Guerrero, E., & Salazar, A. (2014). Comentarios Críticos a la Reforma Del Código Penal que Introduce la Ley 9048 (Sobre Delitos Informáticos en el Derecho Penal Costarricense). *Revista Judicial*, (112), 247-257.

Hernández, L. (2009). El delito Informático. *EGUZKILORE*, (23), 227-243.

Hernández, R., Fernández, C., & Baptista, P. (2006). *Metodología de la investigación* (4ª ed.). México: Mc. Graw Hill.

Hernández, D. A. (2019). *La suplantación de identidad cibernética en el Ecuador.* Tesis para optar por el grado de Maestría. Universidad Externado de Colombia, Bogotá, Colombia. Recuperado de https://bdigital.uexternado.edu.co/bitstream/001/1822/1/GAAA-spa-2019-La_suplantacion_de_identidad_cibernetica_en_el_Ecuador

Hess, C. (2010). Ciberdelitos: tipos y soluciones. En Prosic, *Ciberseguridad en Costa Rica* (pp. 121-131). San José, Costa Rica: Impresiones Gráficas del Este S. A. Recuperado de http://www.prosic.ucr.ac.cr/sites/default/files/documentos/ciberseguridad_2010.pdf

INTECO. (2007). *Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing.* León, España: Autor.

Jara, E., & Álvarez, V. (2008). Desarrollo de las TIC en Costa Rica y su tratamiento en el CAFTA. *Latin American Trade Network LATN*, 1-45. Recuperado de http://latn.org.ar/wp-content/uploads/2015/01/wp-98.pdf

Jiménez, L. (1958). *Principios de Derecho Penal. La Ley y el Delito.* Argentina: Editorial Sudamericana.

La Voz de Galicia. (2014, setiembre 09). ¿Qué son los bots o seguidores fantasmas que asedian el twitter de los políticos? *La Voz de Galicia*. Recuperado de https://www.lavozdegalicia.es/noticia/tecnologia/2014/09/09/bots-seguidores-fantasmas-asedian-twitter-politicos/00031410261277161827597.htm

Lemaitre, R. (2010). *La impunidad de los delitos informáticos en la ciber-seguridad costarricense en el ámbito del Derecho Penal.* San José, Costa Rica. Universidad de Costa Rica

Lemaître Picado, R. (2020). *Manual sobre delitos informáticos para la ciber sociedad costarricense* (2da. ed.). San José, Costa Rica: IJSA.

Licona, A. (2012) Los Medios Informáticos. Recuperado el 29 de enero de 2020 de: http://sac30.blogspot.com/2012/11/los-medios-informaticos.html

López, J., & Torres, M. (2010). *Problemática del Delito Informático: Hacia una necesaria regulación internacional.* San José: Universidad de Costa Rica.

Malware. (s.f.). *Hackeo.* Malwarebytes. Recuperado de https://es.malwarebytes.com/hacker/

Márquez, M. (s.f.). Análisis del delito de usurpación de identidad en México. *Estudios Legislativos,* 335-368. Recuperado de https://repositorio.lasalle.mx/bitstream/handle/lasalle/1422/RA%2033%20Jul2019-335-368.pdf?sequence=1&isAllowed=y

Mata, L. D. (2020). *Métodos y técnicas de investigación cualitativa.* Investigalia. Recuperado de https://investigaliacr.com/investigacion/metodos-y-tecnicas-de-investigacion-cualitativa/

Mata y Martín, R. M. (2003). *Delincuencia Informática y Derecho Penal*. España: EDISOFAR.

Medrano, J. A. (2016, enero 6). Suplantan identidad del Ministro de Seguridad. *Delitos informáticos*. Recuperado de https://adalidmedrano.com/suplantan-identidad-del-ministerio-de-seguridad/2016/

Montaperto, J. E. (2018). *Suplantación de identidad. Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino.* Argentina: Universidad Siglo 21. Recuperado de https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/15652/MONTAPERTO,%20Javier%20Eduardo.pdf?sequence=1

Noguera, Bulmaro (s.f). Cuál es la diferencia entre dato e información. Recuperado el 29 de enero de 2020 de: https://culturacion.com/cual-es-la-diferencia-entre-dato-e-informacion/

Organización de Naciones Unidas. (1996-2020). *Pacto Internacional de Derechos Civiles y Políticos.* NY: Autor. Recuperado de https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx#:~:text=Todo%20ni%C3%B1o%20tiene%20derecho%2C%20sin,la%20sociedad%20y%20del%20Estado.

Pérez, E. M. (julio de 2012). *Sistema de Gestión de Recursos del Centro de Estudios.* Tesis para optar por el grado de Ingeniería Informática. Universidad de Granma, Cuba. Recuperado de http://repositorio.utc.edu.ec/bitstream/27000/1290/1/T-UTC-2041.pdf

Pérez Porto, Julián y Merino, María. (2009) Actualizado: 2012. Definición. de: Definición de operación Recuperado el 29 d enero de: https://definicion.de/operacion/

Poder Judicial. (2017). *Código Penal de Costa Rica.* San José, Costa Rica: Editorial Investigaciones Jurídicas.

Quevedo, J. (2017). *Investigación y prueba del ciberdelito.* Barcelona. Universidad de Barcelona Recuperado de https://www.tesisenred.net/handle/10803/665611#page=1

Quintana, A. (2006). *Metodología de Investigación Científica Cualitativa.* Perú: UNMSM.

Real Academia Española. (2014). *Diccionario de la lengua española* (23ª ed.).

Rivera, V. (2019). Realidad sobre la privacidad de los datos personales en Costa Rica. *E-Ciencias de la Información, 9*(2). Recuperado de https://www.scielo.sa.cr/scielo.php?pid=S1659-41422019000200068&script=sci_arttext

Rodríguez, F. (s.f.). *Derecho informático. El derecho en la era digital. La sociedad de información y el sistema jurídico. Contratos informáticos. Protección jurídica de los programas de computación. Delitos informáticos. La tutela jurídica del sistema informático.* Córdoba: Universidad Nacional de Córdoba. Recuperado de http://www.feliperodriguez.com.ar/wp-content/uploads/2013/11/LIBRO-7-DERECHO-INFORMATICO.pdf

Rogers, D. (2020). *Identidad*. Enciclopedia Jurídica.com. Recuperado de http://www.enciclopedia-juridica.com/d/identidad/identidad.htm#:~:text=(Derecho%20Civil)%20Conjunto%20de%20los,%2C%20filiaci%C3%B3n%2C%20etc.).&text=%7C%20DE%20PERSONA%20o%20PERSONAL.

Romero, R. (2010). *Las conductas vinculadas a la suplantación de identidad por medios telemáticos; una propuesta de acción legislativa*. Ciudad de México, México: Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas. Recuperado de https://archivos.juridicas.unam.mx/www/bjv/libros/6/2941/24.pdf

Roxin, C. (1997). *Derecho Penal. Parte General. Tomo 1*. España: Civitas.

SITEMAP de Tecnología. (s.f.). *Recursos, Conocimientos y Temas de Tecnología*. Autor. Recuperado de https://www.areatecnologia.com/INFORMATICA.htm

Siu, A. (16 de agosto de 2018). *Cómo funcionan los bots (y cómo contribuyen a difundir información falsa).* Red internacional de periodistas. Recuperado de https://ijnet.org/es/story/c%C3%B3mo-funcionan-los-bots-y-c%C3%B3mo-contribuyen-difundir-informaci%C3%B3n-falsa

Soroush, V., Deb, R., & Sinan, A. (2018). The spread of true and false news online. *Science, 359*(6380), 1146-1151. Recuperado de https://science.sciencemag.org/content/359/6380/1146

Soto, M. (2001). La tipificación de los delitos informáticos en la legislación penal venezolana. *Capítulo Criminológico, 29*(3), 101-117.

Taylor, S. J., & Bogdan, R. (2000). *Introducción a los métodos cualitativos.* España: Paidós. Recuperado de https://asodea.files.wordpress.com/2009/09/taylor-s-j-bogdan-r-metodologia-cualitativa.pdf

Téllez, J. (1991). *Derecho Informático.* México: Instituto de Investigaciones Jurídicas.

Vargas, I. (2012). La entrevista en la investigación cualitativa: nuevas tendencias y retos. *Revista Electrónica Calidad En La Educación Superior, 3*(1), 119-139.

Verdugo, A. A. (2011). *Derecho Informático.* Sonora: Universidad de Sonora. Recuperado de http://tesis.uson.mx/digital/tesis/docs/21251/Capitulo3.pdf

Wardle, C. (2017). *Noticias falsas. Es complicado.* First Draft. Ed. Recuperado de https://es.firstdraftnews.org/2017/03/14/noticias-falsas-es-complicado/

Wardle, C. (2019). Understanding Information Disorder. Berlin, Germany: First Draft Publishing. Comprensión del trastorno de la información. Berlín, Alemania: Publicación del primer borrador. Recuperado de https://firstdraftnews.org/wp_content/uploads/2019/10/Information_Disorder_Digital_AW.pdf?x76701

ANEXOS

Anexo N°1. Instrumento de consulta-entrevista operadores del derecho y la informática.

Dirigido a abogados defensores, para identificar aportes vivenciales en el abordaje de los delitos informáticos en el marco jurídico costarricense, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente José Benjamin Hidalgo Durán, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista realizada al Lic. Pablo Rojas Arias. Abogado defensor.

1) ¿Qué es un ciberdelito o delito informático?

-Actualmente la normativa es muy amplia, como han catalogado los ciberdelitos informáticos aquellos en los que se dé la utilización de medios informáticos, o medios de acceso alguna red, no entendida únicamente como la llave para la realización del delito sino inclusive entendido como de acceso a la información, utilización simple de algún dispositivo electrónico para la realización del delito, que en buena teoría se esperaría que no fuera así, pero ha sido muy amplio se ha dado la apertura de los tipos penales o de los elementos objetivos de manera amplia, considero al menos haga en Costa Rica.

2) ¿Cuál es el perfil de quien comete delitos informáticos?

-En lo que tenemos día a día no hay ningún perfil definido, porque gracias a esa amplitud de elementos objetivos que se han dado cualquier persona ha sido catalogada en la normativa o en los procesos penales como una persona que podría llegar a cometer un delito informático, ya que gracias a que no existe esa determinación personalizada incluso se tienen indigentes que pasan por delitos informáticos simple y sencillamente porque se les abrió una cuenta y se les deposito un

dinero, actualmente no hay un perfil de delincuente informático al menos eso es lo que he percibido.

3) Según su experiencia ¿cuáles son los delitos informáticos más frecuentes que se cometen?

-Actualmente según la experiencia propia eso variar mucho según la jurisdicción que este uno esté trabajando, en todas hay perfiles de delitos que se trabajan.

-Al menos en Cartago y San José lo que se da es el fraude informático, llamado la estafa triangular, que se le denomina así por parte del Ministerio Publico donde se hace la llamada, se logra la extorción del dinero y posiblemente se deposita a terceras personas, ese es el delito más común en ambos lugares y otro de los delitos informáticos que podría darse es la difusión de pornografía en redes sociales o intercambio inclusive de organizaciones que se dedican a vender las imágenes sexuales incluso de personas menores de edad actualmente esos son los delitos que más se dan. -No he tenidos delitos de suplantación de identidad o de exposición de datos falsos.

4) ¿Es difícil identificar a los sujetos activos de los delitos informáticos?

-Sí, de hecho que yo creo que el tipo penal actualmente se está aplicando de manera errada porque a las personas que pasan como te decía, son las personas finales donde el dinero termina que en muchas ocasiones esas personas no saben cuál es el origen del dinero son personas que son engañadas o se les pide como un tipo de favor o con información falsa en donde lo que le dicen es que mira necesito que prestes la tarjeta y nunca se enteran de cuál es el origen del dinero sin embargo lo hacen desconociendo para qué fue que se utilizó la cuenta.

-Esas son las personas que tenemos como usuarios penales en nuestro sistema que estoy cien por ciento seguro que esas personas que se están procesando por ese delito ni si quiera cumplen con los parámetros de los elementos objetivos del tipo penal, ellos nunca llegan a

manipular un sistema, nunca llegan a extraer la información de la parte ofendida, ni si quiera saber cuál fue el origen de ese dinero y eso ha generado que tengamos una taza alta de delitos pero que realmente nunca han determinado quien fue la persona, cual fue el medio que se utilizó, cual computadora se utilizó, entonces la dificultad se presenta en que los cuerpos policiales, el OIJ y el Ministerio Publico actualmente no están preparados para perseguir ese tipo de delitos, inclusive cuando se lograra identificar a la persona que extrae la información eso para mí, no cataloga como un delito de estafa informática, porque la información con la que se está accediendo es una información real que se extrajo por medio de un engaño, pero la llave que se está utilizando para ingresar a los sistemas informáticos es la llave correcta que cualquier persona utilizaría, una comparación sería lo mismo cuando hablamos de un robo agravado o inclusive un hurto agravado cuando se indica que se utilizó una ganzúa para abrir una puerta si yo utilizo la llave correcta para abrir una puerta cuando esto pasa no hay un agravante, hay un hurto común y corriente porque se está utilizando la llave que comúnmente se utiliza es por eso que yo considero que no se cumplen con los delitos de estafa informática como tal ya que se utiliza información verdadera extraída a través de un ardid de un engaño y ahí radica la dificultad de perseguir el delito como tal.

5) ¿Cuál es el mayor problema judicialmente a la hora de afrontar un proceso judicial por este tipo de delitos?

realmente creo que gracias a esta ausencia de investigación o que no estamos preparados para perseguir este tipo de delitos la problemática no ha sido tan grave ya que la mayoría de esos casos terminan en sobreseimientos, ya que la persona que defendemos llega con una justificación que no puede ser derivada por parte del Ministerio Publico llegamos y le decimos, bueno si efectivamente yo tengo un depósito en mi cuenta pero este depósito tiene varias explicaciones de porque llego ese dinero entonces esto no pueden ser derivadas.

-El problema que se presenta es que es un cambio normativo que tiene que respaldarse y esos respaldos se hacen no solamente a través de política criminal del Ministerio Publico sino que hubo una asamblea que impulso esos cambios esa nueva ley a aplicarse, hay una nueva presión internacional en donde los delitos informáticos están dando de qué hablar a nivel internacional, y el país tiene que dar resultados, actualmente a nivel procesal el problema se presenta por la respuesta social que tenemos que dar ante un delito que está siendo impulsado por un país en donde tiene que dar resultados pero a nivel de la tramitología del expediente con las investigaciones que se presentan y lo digo con los delitos que conozco, creo que en un proceso apegado el derecho, apegado a elementos probatorios reales, apegado a un análisis objetivo del juez casi que ninguno debería llegar a la etapa de debate, sin embargo hay una presión social que hace que algunos lleguen a juicio y sean condenados pero mal condenados porque las pruebas no dan para ello. Pero hay que dar una respuesta social y política de esta inserción de tipos penales que se hizo en nuestra normativa.

6) ¿Cuáles son los principales problemas o impedimentos para poder procesar a una persona que comete un delito informático?

-Yo creo que tengo que darle la misma respuesta el OIJ y el Ministerio Publico no están preparados y esta preparación va de la mano de la ausencia de ligámenes o coordinaciones que se puedan hacer especialmente con las entidades bancarias, porque ni si quiera las entidades bancarias están preparadas para alertar ese tipo de inclusiones que se le hacen a sus sistemas a cuentas de sus usuarios, precisamente porque el acceso con el que se ingresa a las cuentas del ofendido, es el acceso correcto y reamente los bancos no tienen sistemas especializados de este tipo de intromisiones que se hacen porque muchas de las denuncias que llegan al OIJ serían fácilmente detectables por los bancos.

-Cómo es posible que un banco por ejemplo en mi cuenta normalmente yo hago transacciones nada mas de giros comerciales en pulperías o establecimientos determinados, el banco no determina o no activan alertas cuando se haga una un transacción a las diez de la mañana de doscientos mil colones, a las diez y treinta otra de doscientos cincuenta mil colones, a las tres de la tarde otra de quinientos mil colones a distintas cuentas, yo creo que esa alerta debería activar las entidades bancarias y la entidades bancarias tener un ligamen directo con el OIJ, en ese momento la participación ya de investigación judicial es donde debería ser efectiva, sin embargo se da días después cuando la persona usuaria determina que se realizaron las transferencias o en ese mismo día le llegan todas las notificaciones a las cinco de la tarde, cuando ya se pasaron todo el dinero, esta persona acude al sistema judicial al día siguiente y hace la denuncia, pero ya los dineros están depositados ya, si se hizo desde un café internet ya la persona no está ahí, entonces creo que ***la dificultad para la persecución es la ausencia de herramientas para la detección inmediata***.

-Otra de las dificultades es la ***reacción tardía*** que tiene el OIJ que es el que tiene que investigar ya cuando un delito este cometido entonces es una reacción tardía al fraude informático.

7) ¿La terminología del tipo penal, crea algún problema que se habla de phishing, hardware, software?

-El asunto es que normalmente los delitos, que se tipifican a nivel costarricense se adecuan a una conducta, entonces se genera el tipo penal, un ejemplo muy claro es por ejemplo esta ley de acoso callejero, que muchas denuncias empezaron a llegar en donde decían es que me persiguen, es que he visto muchas personas masturbándose, las conductas eran descritas en distintas normas, en donde lo que se hacía era pasarlas al contravencional porque no era delito, pero entonces se

tenía una descripción casi que especifica de ***cuál era la conducta que se pretendía perseguir***, entonces después se hizo una figura penal narrando cuales eran las conductas de interés.

-En el caso de los delitos informáticos, como es un asunto que a nivel costarricense no ha tenido el peso ni ha tenido la denuncia ciudadana, lo que se hizo fue distinto fue hacer un tipo penal para tratar de que las posteriores conductas encuadraran en esos elementos objetivos, entonces la terminología utilizada son términos en los que tratan de englobar conductas que todavía no se han tenido en la práctica, entonces evidentemente al ser un delito especializado, tiene que utilizar términos especializados de la rama de la informática, pero a nivel de tipos penales de la tipología de la determinación del delito debió hacerse más amplia en el sentido de que se explicara que es el phishing, que es la persona que pone el anzuelo para que la víctima caiga a nivel de redes sociales, todo eso se debería de explicar así tan específicos pero el problema se presenta porque lo que se hizo fue primero la figura penal para tratar que después las conductas encuadren ahí y no como normalmente se hacen los delitos acá en Costa Rica, la terminología ha generado que conductas que son de la normalidad, conductas que podrían encuadrar en otros tipos penales se agarren y se metan ahí para tener un circulante de delitos informáticos, cuando creo que no son delitos informáticos.

8) ¿Considera usted que el abogado debería especializarse a nivel de licenciatura o dar las universidades la materia de delitos informáticos ya que va en crecimiento y no se va a detener?

-Sí, evidentemente el derecho es cambiante, usted como abogado tiene que estar siempre actualizado no sé si desde las universidades, ya que las universidades deberían de ampliarse en muchas cosas antes de pensar en esto que es tan novedoso, pero si el abogado tiene que especializarse cuando ya esté definido cuál va a ser su materia y su rama de aplicación del derecho

y más bien debería ser especializaciones que se impulsen desde el colegio de abogados y tal vez no de las universidades que deberían únicamente insertar a los estudiantes en la existencia de este tipo de delitos, pero ya la capacitación que el abogado tenga se debe de hacer cuando ya haya definido su rama de investigación, es evidente que va en crecimiento pero la especialización tiene que venir de la motivación y de la dedicación que cada profesional tenga a lo que se vaya a dedicar. Los delitos informáticos no están en mi prioridad en mi caso.

9) Con respecto a los ciber delitos y delitos informáticos ¿qué recomendaciones daría para mejorarlo?

- De nuestra parte no interesaría que mejore mucho, ya que esas son falencias que nosotros utilizamos para defensa del usuario que nosotros tenemos pero si realmente hay alguna motivación en perseguir ese tipo de delitos, lo que tiene que ocurrir es una ***alianza fuerte*** del OIJ con las entidades bancarias en donde la posibilidad de determinar la sustracción de dineros casi que se dé inmediata, seguidamente la ***especialización de equipos*** en el OIJ y la unidad especializada que vallan a crear, ya se está gestionando una fiscalía de ciberdelincuencia, y evidentemente la ***capacitación para las personas*** que vayan a trabajar en ese tipo de delitos es primordial, monitoreo efectivo de la posibilidad de poder determinar los IPES de manera automática, la posibilidad de poder rastrear usuarios tanto nacionales como internacionales, alianzas que se puedan hacer con cuerpos policiales internacionales. Si quieren fortalecer esta persecución a nivel de ciberdelincuencia necesitamos alianzas necesitamos equipo y necesitamos capacitación.

10) ¿Cuáles son los problemas de los tipos penales?

-El problema es que hicieron la figura penal para tratar de encuadrar conductas en esa figura penal y no definir una conducta que ya estaba ocurriendo y tipificarla, sino que se hizo al revés se tipifico y se tratan de meter conductas, por ahí viene el problema ya que resulta ser que este tipo

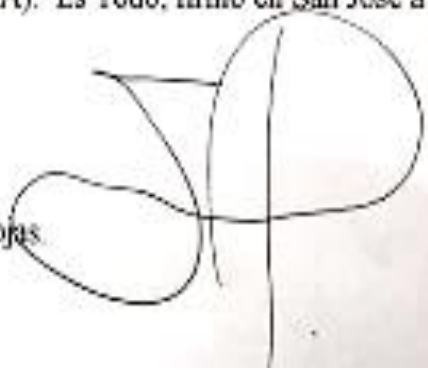
penal de estafa determina la posibilidad de manipular, ingresar, insertar en un sistema informático, utilizar datos falsos con la finalidad de tener un beneficio económico, esos son los elementos objetivos específicos de mayor importancia de ese tipo penal, pero lo que actualmente tratamos es una estafa común y corriente en donde lo que se utilizó para sacar el dinero fue la misma clave que usted brindo y se hizo un depósito a una tercera persona, por lo que no habría ninguna intromisión errónea de datos falsos, no hubo ninguna manipulación por parte de un tercero de manera errada, se utilizó una herramienta para que usted pusiera los datos que necesitaba, aunque muchas veces usted mismo los brinda por vía telefónica, ese es el problema que se está metiendo conductas normales de una estafa normal en este tipo informático y no lo es.

-Un ciberdelito o un delito informático debería de perseguir las intromisiones erradas que se hagan en sistemas, todavía sería más partidario en aquellos casos en donde lo que se demanda, son estas páginas falsas que extraen la información del usuario hay podría darse un delito de estafa informática, sin embargo no he tenido ninguna en esa modalidad lo que se está atendiendo actualmente son las sustracciones por vía bancaria, ***el problema va en la necesidad del estado de dar una respuesta de que se están obteniendo resultados pero que no se está utilizando el tipo penal como debería de utilizarse.***

Consentimiento informado Lic. Pablo Rojas Arias. Abogado defensor.

CONSENTIMIENTO INFORMADO

Yo Juan Pablo Rojas Arias, con cédula de identidad número: _1-1224-0747, autorizó que se ponga mi nombre, que se grave mi voz, para efectos de la investigación, la cual es: LA ESPECIFICIDAD DE CONOCIMIENTOS EN LOS DELITOS INFORMÁTICOS, del estudiante: JOSE BENJAMIN HIDALGO DURAN, cedula de identidad número: 205050745, de la Maestría de Derecho Penal, de la Universidad Internacional de las Américas (UIA). Es Todo, firmo en San José a las 12:00 horas del día 08 del mes de Enero de 2021.



Juan Pablo Rojas

Dirigido a abogados defensores, para identificar aportes vivenciales en el abordaje de los delitos informáticos en el marco jurídico costarricense, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente José Benjamin Hidalgo Durán, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Lic. Francisco Cerna. Abogado defensor.

1) ¿Qué es un ciberdelito o delito informático?

La legislación costarricense, lo que trata es de tutelar en base al ciberdelito, es cualquier acción en contra de algún sistema informático que cause algún perjuicio patrimonial por ejemplo en el caso de los bancos sea perseguido de forma especializada mediante un tipo penal privilegiado.

2) ¿Cuál es el perfil de quien comete delitos informáticos?

-Usualmente son personas que conocen sobre la materia informática, no necesariamente deben tener algún estudio, simplemente que si tengan conocimientos de sistemas o de programación con el efecto de tratar de vulnerar los sistemas informáticos.

3) En el caso de las estafas las personas que llegan a ser procesadas ¿son ingenieros informáticos o no necesariamente?

-No necesariamente, lo que se necesita es un conocimiento empírico, usualmente son ingenieros o algún tipo de la rama informática, las personas encargadas, no obstante, como le reitero más bien son conocimientos empíricos o talento incluso innato de las personas para los efectos de vulnerar los sistemas informáticos.

4) ¿Cuáles delitos se cometen más o se llevan a los tribunales?

-Usualmente son los fraudes con tarjetas de crédito o con tarjetas de débito, que son las estafas informáticas, donde una persona ya sea mediante cárcel u personas afuera se hacen las llamadas, las tradicionales llamadas de estafas, hackean el sistema informático en base a los datos que la gente proporciona induciendo al error y posterior de ello tratan de conseguir personas que

se le denominan frentiadores que son las que prestan las cuentas bancarias ya sea con conocimiento o sin conocimiento igualmente inducidas a error para los efectos que sean ellos finalmente perseguidos penalmente dado que son los titulares de la cuenta bancaria donde se retiró el dinero y donde usualmente son las personas que se observan en las cámaras de seguridad de los cajeros automáticos haciendo el retiro.

5) Según su experiencia ¿cuáles son los delitos informáticos más frecuentes que se cometen?

-Precisamente son los que mediante la ictericia o falta de cuidado de las personas suministran datos, les hacen el hackeo de la información bancaria y les hacen un retiro de dinero.

6) ¿Es difícil identificar a los sujetos activos de los delitos informáticos?

-Normalmente es un delito tripartito, quiere decir que es un delito de la persona que llama induce a error y extrae la información de la persona, que comúnmente son personas que se encuentran en los centro penales con facilidad de dialogo, posteriormente el hacker, que es la persona que realiza el trámite informático y que realiza el débito del dinero y el traslado del mismo y posteriormente la persona frentiadora que es la que usualmente se le imputa dado que es la única persona con la cual se tiene un elemento de prueba los cuales son la cuenta bancaria dónde cae el dinero y posteriormente se retira.

Usualmente lo que es el hacker y la persona que llama, la policía costarricense actualmente no cuenta con la tecnología necesaria como para tratar de ubicar de manera informática el email o algún tipo de hipervínculo para tratar de localizar esta persona hacker y eventualmente en igual sentido cuesta mucho hallar ya la información telefónica de la persona que realiza la conversación que induce a error al ofendido.

7) ¿Cuál es el mayor problema judicialmente a la hora de afrontar un proceso judicial por este tipo de delitos?

-De parte de la defensa, el contratiempo usualmente o más bien puede verse como dos cosas o a favor o en contra, a favor seria la imposibilidad de acreditar la forma dolosa de que la persona retiro con conocimiento de hecho el dinero, usualmente esa es la estrategia que se utiliza normalmente salvo casos excepcionales, donde cada caso tiene su forma de ver las cosas pero usualmente lo que utilizamos es la falta de elementos de prueba para acreditar el dolo que es el conocimiento y voluntad de la persona para realizar la extracción de dinero, eso se plasma con una declaración indagatoria bien estructurada donde efectivamente la persona determine si fue un favor, fue un tipo conocido donde existía ese nivel de confianza como para realizar ese favor.

8) ¿Generalmente, terminan sobre seguimiento o no continúan?

-No, Usualmente la persecución penal por parte del Ministerio Publico por un tema estadístico normalmente sigue, se la acusa a la persona, pero si se trabaja bien, usualmente tiene un final prometedor para la defensa en razón desde que un principio mostro la defensa de que no existía ningún tipo de conocimiento o voluntad para los efectos de la realización de ese hecho delictivo

9) ¿Según su experiencia en caso de existir problemas cuales son los principales obstáculos para procesar penalmente a los delincuentes informáticos es decir a los ingenieros, a la gente que está en las computadoras o generalmente no se ve eso?

-Usualmente como se lo dije líneas atrás uno de los mayores impedimentos es que Costa Rica por lo menos a nivel de investigación se encuentra en pañales, en los ciberdelitos de hecho Costa Rica no tiene un sistema policial o peritos que vengan a determinar por medio de los IP, email o cualquier dato que sea diminuto informático para los efectos de dar con el equipo

informático y así mismo con el dueño de ese equipo informático para los efectos de determinar el hacker incluso existen problemas con las cripto-monedas que Costa Rica está en pañales de la individualización de este tipo de delincuencia.

10) ¿Deberían los abogados prepararse en esa materia de delitos informáticos?

-Bueno, una de las cosas es que los abogados nunca tenemos un conocimiento total de todas las materias, es responsabilidad de todo profesional irse actualizando como un médico.

-Recuerde que el derecho es una ciencia social, al ser una ciencia social pues evoluciona como tal, estamos ante una era informática por consiguiente los delitos se van a ir estilizando hacia esa bancada.

11) ¿Qué considera usted que se debería mejorar, frente a la persona que ha sido vulnerada en sus cuentas bancarias, que se debería mejorar según su experiencia en la persecución de este tipo de delitos?

-Eventualmente existe un canal informativo, tanto del OIJ como de televisoras donde instan a las personas a no prestar en ninguna circunstancia cuentas bancarias, a partir de ahí sería una información más globalizada y crear una cultura ante esa situación en base a eso pues el riesgo disminuiría considerablemente bajo este tipo de hechos delictivos, entonces concientizar y cultivar a la población en este sentido.

Propiamente dotar al Organismo de Investigación Judicial de peritos propios y aptos en la materia para los efectos de desarticular las bandas.

Prevenir, no reprimir, seria llenarse de conocimiento, experiencia para realizar seguimientos de bandas organizadas para los efectos de tener el tiempo suficiente de confeccionar una buena investigación y no de forma prematura fulminar un caso que tal vez hubiera dado un resultado de mayor impacto y de forma positiva y no de forma prematura por un tema de estadística

12) ¿Existe algún problema con el tipo penal de la estafa, por ejemplo, que es el que ustedes más ven, en cuanto la tipicidad o la formalización del artículo?

-Bueno ahorita no tengo el código a mano, ahí sí sería muy irresponsable ya que no se me el tipo penal de memoria, entonces esa pregunta prefiero no abarcársela.

13) ¿Existe algún problema a nivel de investigación o del mismo proceso en cuanto al lenguaje que se utiliza en la informática por ejemplo phishing, hardware, software, hacker?

-Evidentemente el abogado debe prepararse para comprender el lenguaje, en primer lugar como cualquier otro caso o en la materia que se desempeña llámese informático o una administración fraudulenta, pues uno debe de preparar su contabilidad evidentemente no va a tener desenvolvimiento como un profesional de esa área, pero si debe tener que cultivarse para los efectos de enfrentar el caso, también la ley le otorga la posibilidad de tener ya sea peritos o consultores técnicos que son los profesionales de la materia para así tratar de abarcar esas ramas de una materia más científica.

Consentimiento informado Lic. Francisco Cerna. Abogado defensor.

CONSENTIMIENTO INFORMADO

Yo Francisco Cerna M. **, con cédula de identidad número:** 6-380-124 **, autorizó que se ponga mi nombre, que se grave mi voz, para efectos de la investigación, la cual es: LA ESPECIFICIDAD DE CONOCIMIENTOS EN LOS DELITOS INFORMÁTICOS, del estudiante: JOSE BENJAMIN HIDALGO DURAN, cedula de identidad número: 205050745, de la Maestría de Derecho Penal, de la Universidad Internacional de las Américas (UIA). Es Todo, firmo en San José a las 10:00 horas del día xxx del mes de Diciembre de 2020.**

FIRMA Digital.

Dirigido a abogados defensores, para identificar aportes vivenciales en el abordaje de los delitos informáticos en el marco jurídico costarricense, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente José Benjamin Hidalgo Durán, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Lic. Joffre Montero Zúñiga. Abogado defensor.

1) ¿Qué es un ciberdelito o delito informático?

-Bueno, un ciberdelito o delito informático son delitos que el legislador estableció como figuras delictivas, que contemplan el resguardo de algún tipo de base de datos o de información, usualmente van a ser delitos en donde lo que se vulnera, es algún sistema informático, algún sistema de datos, una base digital que contenga datos, entonces básicamente es eso delitos que resguardan o el bien jurídico que protegen es datos o información, que usualmente suelen estar contenidos en lo que se llama contenedores magnéticos, contenedores de almacenamiento, memorias, discos duros, plataformas de información, un delito informático, es un delito que se comete contra la información en términos generales, el contenido con el que cuentan en la actualidad es información que se encuentra digitalizada de alguna manera o que se encuentra en bases informáticas.

2) ¿Cuál es el perfil de quien comete delitos informáticos?

-Para contestarle eso, debo de hacer una disgregación o una disección entre lo que sucede en la realidad que son las personas en las que finalmente terminan siendo imputados y los que realmente inciden en las bases de datos, que son personas muy diferentes, lo que quiero explicarle con esto, es que es que el perfil que uno observa en los tipos penales que describen en los delitos informáticos requieren que la persona que los vaya a cometer tenga ciertos conocimientos especializados, por ejemplo el manejo de bases de datos, de sistemas informáticos, de sistemas de programación, son personas que tienen un tipo de preparación en aspectos informáticos, lo cierto

del caso es que en la práctica en realidad quienes terminan siendo imputados de este tipo de delitos no son usualmente las personas que realizan esas maniobras de incidir sobre bases de datos o programas, porque en realidad a los que terminan procesando penalmente son personas que por ejemplo, el delito informático se puede dar por medio de utilización de información de manera errónea, maliciosa por incidir en bancos de datos y demás, pero resulta ser que las personas que inciden en esos datos en realidad no son los que terminan siendo procesados sino son las personas que finalmente se presentan en los bancos a retirar los dineros, no sé si usted ha tenido la oportunidad de tener alguna experiencia con este tipo de delitos, básicamente alguien pesca los datos del ofendido, que son los de ingreso a una cuenta de banco, sacan el dinero de esa persona y posteriormente se encargan de reclutar a terceras personas que son las que terminan sacando el dinero, usualmente el perfil de estas personas es de baja escolaridad, urbano-marginales, quienes lo hacen a cambio de algún tipo de beneficio de dinero, en ocasiones pueden que sepan que es un delito en otras no inclusive son engañados que podría ser de las cosas que se puede alegar, es decir que si, si cuenta se utilizó para pasar fondos que habían sido ilícitamente obtenidos pero esta persona no sabía que eso era así, entonces cuando usted me pregunta por el tipo de perfil de las personas que cometen este delito son los que inciden en el procesamiento de las bases de datos son personas que tienen una capacitación en el manejo de sistemas de información pero se sirven de otras personas para lograr sacar el dinero del sistema bancario, siempre se necesita de varias personas. Los hackers tratan de no dejar ningún rastro tanto informático como físico.

3) Entonces ¿la persona que comete el delito desde la computadora es difícil rastrearlo?

-En el tiempo que tengo de ser defensor público, que son diez años solamente en una ocasión recuerdo que agarraron a la persona que era un ingeniero en sistemas que era el que incidía en la base de información.

No es cualquier persona que puede hacer una página idéntica de un banco para que una persona cometa el error de ingresar sus datos exactamente iguales y así es como obtiene los datos de las personas o bien envían correos electrónicos a muchísimas personas con logos y cosas que parecen ser autorizados del banco, entonces ellos introducen en ese correo electrónico todo lo que les están pidiendo claves, contraseñas y demás y cuando se dan cuenta que le hicieron inteligencia social a las personas víctimas, obviamente ingresan automáticamente a las cuentas y las vacían.

Hay un software que se conoce como VPN que permite que las personas que cometen estos delitos, utilicen técnicas de anonimización las direcciones IP y desde donde están realizando un hecho entonces se podría estar en Costa Rica pero usted lo puede modificar que se está realizando desde China, entonces cuando la policía intente verificar de que IP se hizo para buscar la computadora y para poder ubicar a un posible autor del delito en realidad nunca lo van a poder encontrar entonces solo queda las personas que prestaron su cuenta para depositar el dinero y ellos extraerlo siendo los únicos que quedan expuestos.

4) Según su experiencia ¿cuáles son los delitos informáticos más frecuentes que se cometen?

-Sí, el más frecuente es la estafa informática, lo que son los otros delitos como suplantación de identidad o algunos de los delitos que tienen que ver con los tipos penales que están contemplados como la facilitación de delitos informáticos, suplantación de páginas electrónicas, espionaje o el sabotaje informático son delitos que, no son tan comunes.

5) ¿Es difícil identificar a los sujetos activos de los delitos informáticos?

-Sí, de las cuestiones que más dificultan la investigación en este tipo de delitos, es la técnica de anonimicen que utilizan que son muchísimas, de lo que uno ha visto en las prácticas y les ha tocado estudiar las técnicas de anonimizaron son muchísimas, muy variadas además de eso les permiten un anonimato a la persona que los está realizando de hecho se realizan de muchísimas maneras por ejemplo por medio de una VPN, se pueden cometer montones de delitos que inclusive están por fuera de las posibilidades estatales, que son los ingresos atreves de la web o la web oscura que se comete cualquier cantidad de delitos, en la web profunda es decir el internet que nosotros conocemos es tan solo una forma de compartir información a nivel global pero existen otras formas entre esas están la Deep web que es una manera de ingresar a paginas prohibidas donde se venden órganos, armas, drogas para acceder una página de internet uno ingresa con una dirección de dominio tipo: www o http, esos son dominios que son utilizados a nivel mundial pero hay otros dominios que se ingresan a través de esta web oscura, que le permite a la gente traficar cualquier tipo de objeto de índole delictiva, yo no sé si usted conocía eso, algo se ha visto de los estudios de otras tesis, no se conoce el detalle.

De hecho que yo no sé si usted ha visto un iceberg, la forma que tienen, la parte que se logra observar por encima es más pequeña de lo que hay por abajo, algo así es la comparación que hacen con la web normal que nosotros conocemos o la web oscura, se dice que los informáticos han definido que la cantidad de web oscura son muchísimas más de las que nosotros conocemos en la web normal, es otro sitio fácil para cometer delitos ya que no queda nada registrado, de hecho los que ayudan a registrar desde donde fue que se realizó un determinado movimiento esos son las plataformas de servicios, que son ICE movistar, ellos son los que realmente le permiten determinarlo con un número, pero con VPN usted puede hacer que ni el mismo ICE sepa lo que usted está haciendo en un determinado momento.

6) Según su experiencia, en caso de existir problemas, ¿cuáles son los principales obstáculos para procesar penalmente a los delincuentes informáticos?

-Un obstáculo es la anonimización.

-La posibilidad que tienen de anonimizar las IP y borra todos los rastros informáticos.

-La dinámica compleja que reflejan estos hechos delictivos, desde la perspectiva que se pueden cometer en cualquier parte del mundo ya que lo comete atreves de la web.

-La internacionalización de los delitos lo complicado que resulta de alguna manera ya que si un fiscal de Costa Rica quisiera investigar un hecho donde se tiene una IP domiciliada en alguna parte del mundo va a necesitar solicitar a la policía que le ayude a recabar esa prueba que se hizo allá implica verificar legislación de otros lados si se puede pedir la información igual como se pide en Costa Rica, esos son serios delitos, aparte que parece que todos estos delitos se dan mediante un contexto de globalización de la información, ya no hay fronteras que puedan ser un obstáculo para una persona ya que no se necesita la presencialidad física para cometerlo entonces esta dinámica es un obstáculo importante.

-Otra problemática importante, es lo desfasados que están de alguna manera los sistemas de investigación al menos en la experiencia de Costa Rica, que es lo que podemos hablar es decir la policía de investigación no tiene las herramientas tecnológicas para poder des mascarar este tipo de delitos, de acuerdo a las posibilidades que tienen más bien los delincuentes de delitos informáticos, lo que quiero decir es que las herramientas investigativas que tiene la policía se quedan cortas ante la gran capacidad y la gran posibilidad que tiene los delincuentes informáticos

-Otra de las cosas importantes, es que el acceso a la información no es tan fácil, se necesitan convenios internacionales, de hecho, está el convenio internacional de Budapest sobre ciberdelincuencia, que permite que sobre los estados se puedan compartir información a nivel

policial, por ejemplo, si yo tengo un IP domiciliada sospechosa debo de empezar porque el país haya firmado el convenio para poder hacer solicitud de información de este tipo.

6) ¿La terminología del tipo penal en delitos informáticos, que se yo, que se habla de un lenguaje muy informático por ejemplo de phishing, hardware, software, hacker es algún impedimento?

-Pues no me parece, pues un tema que va implicar que el operador del derecho tenga que profundizar sus conocimientos en la materia, estudiarlos, no quedara de otra por lo que no me parece que eso sea un inconveniente le soy sincero, ¿porque? porque es como que usted me diga a mí que algún delito económico tenga por ejemplo un informe contable ya que para eso existen los peritos que pueden darle un auxilio en las partes del proceso, obviamente desde el momento que algún tipo penal contemple alguna terminología informática, pues el operador del derecho está en la obligación de determinar concretamente, ya que eso le va a permitir establecer cuál es el núcleo de la figura delictiva.

7) ¿Deberían de estar concentrados los delitos informáticos, en un solo apartado en una sola ley o a como están, están bien?

-Por orden pues sí, sería lo conveniente, en nuestro caso nosotros tenemos solamente el 2 17 BIS que es sobre estafa informática que es el que esta aparte en delitos de contenido patrimonial , los demás delitos si están en la sección octava de los delitos informáticos con nexos pero el orden no altera el producto por decirlo así en sentido mientras que estén descritos este correctamente escritos sería suficiente, ahora puedo decir que los tipos penales que nosotros tenemos no son muy claros, tienen errores en términos relevantes, algunos no diferencian entre datos e información que son cosas diferentes.

8) ¿Deberían las universidades preparar a los estudiantes de derecho en delitos informáticos o cibercrimen, tener una especialización más detallada a nivel de licenciatura?

-No me parece, no creo que deban tenerlo en realidad, le voy a decir porque, porque en licenciatura el objetivo que debe tener una universidad es que las personas salgan con los conocimientos más básicos sobre cada una de las materias más importantes derecho público, derecho privado y los derechos que han tenido más desarrollo una persona por ejemplo va a estudiar derecho penal como tal digamos que quiera hacer la especialización si me parece importante pero ya a nivel de postgrado. Por ejemplo, en penal me parece más importante que una persona maneje teoría de delito y desde procesal maneje las pruebas las más convencionales que tenga un manejo habilidoso de delitos informáticos.

9) Con respecto al tema de los ciberdelitos y el procesamiento penal en Costa Rica ¿qué recomendaciones considera para mejóralo?

-Procesales, para mejorarlo podría ser este tipo de delitos requiere una acción más inmediata, que la respuesta sea más inmediata, no es poco común más bien es muy común que estos delitos se investiguen hasta tiempo después, tal vez que la respuesta sea más inmediata porque el tiempo es algo que le puede servir a las personas que utilizan este tipo de sistemas de información para encubrir, de alguna manera, el rastro de forma más fácil.

En realidad recomendaciones a título así como procesales no veo más allá talvez lo que pienso es que los aparatos de investigación nuestros puedan talvez explorar, hacer gestiones a nivel internacional, digamos algún delito que se comete por la plataforma de Facebook tenga la posibilidad de tratar de tener convenios para tener un acceso a la información más rápida lo que pasa es que no es tan fácil, en Facebook hay políticas de privacidad que obligan que no se puede dar información a cualquier persona, pero si talvez un sistema más amplio con la investigación

10) En cuanto a la tipicidad de los delitos informáticos por ejemplo el de estafa ¿hay algún problema?

-Si claro, es un tipo penal sumamente amplio, ya que contiene una cantidad de modalidades que lo hacen sumamente amplio por ejemplo uso de datos falsos, uso de datos incompletos por programación valiendo de una informática o de un artificio. Acuérdese de uno de los principios de derecho penal es la ley estricta en tema de tipicidad y delitos penales, de hecho, el tipo penal de estafa informática si usted lo va a tener un montón de elementos coincidentes ya que contiene tantas descripciones que lo hace ser muy amplio**.**

Consentimiento informado Lic. Joffre Montero Zúñiga. Abogado defensor.

CONSENTIMIENTO INFORMADO

Yo Joffre Sebastian Montero Zúñiga **con cédula de identidad número:** 1-1294-0386, **autorizó que se ponga mi nombre, que se grave mi voz, para efectos de la investigación, la cual es: LA ESPECIFICIDAD DE CONOCIMIENTOS EN LOS DELITOS INFORMÁTICOS, del estudiante: JOSE BENJAMIN HIDALGO DURAN, cedula de identidad número: 205050745, de la Maestria de Derecho Penal, de la Universidad Internacional de las Américas (UIA). Es Todo, firmo en San José a las 10:00 horas del día** 07 **del mes de Diciembre de 2020.**

FIRMA Digital.

Dirigido a abogados Litigantes, para identificar aportes vivenciales en el abordaje de los delitos informáticos en el marco jurídico costarricense, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente José Benjamin Hidalgo Durán, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Lic. Henry Angulo Yu. Abogado Litigante.

1) ¿Qué es un ciberdelito o delito informático?

-Por ser un área nueva, la mayoría de las personas contamos con acceso a internet por medio de celulares, computadoras, en especial hay un tema con los celulares que está democratizando muchísimo este acceso a internet, es un aspecto sumamente difícil de definir, hay una infinidad de autores que han tratado de llegar al asunto algunos por opciones más amplias otros por más restrictivas, por otra parte algunos consideran delito informático a aquella acción jurídica y culpable, en la cual por medio de computadoras para esas personas el simple hecho de que exista un equipo de procesamiento de datos sea suficiente para considerarlo un delito informático, hay otras personas que consideran que no es solo aquel delito cometido por computadoras sino que es la computadora sea el objeto como tal de ese delito.

-Don Francisco Castillo, no trataba de definir el delito como tal sino de conceptualizarlo teniendo una de las visiones más aceptadas a mi criterio, llega a reconocer que el calificativo informático es sumamente amplio y que a partir de ahí tenemos que empezar a escribir acciones más estrictas para aplicarlo a lo jurídico, termina comentando que hay un tema informático amplio, como aquel delito que se cometa por medios informáticos y en el sentido estricto don Francisco señalaba que es el medio fundamental con el cual se comete el delito queda siempre el hecho que se utilizó una computadora para falsificar el cheque ¿es eso delito informático o no? Para algunas personas si vendría siendo un delito en este caso casi que todos los delitos serian informáticos ya que todo lo manejamos con equipos de procesamiento de datos ya que todo se maneja de manera

autónoma, si hay que buscar aspectos más estrictos para poder aplicar esto al contexto del derecho y más allá de todo esto cabe preguntarse si vale la pena definir estrictamente que es un delito informático como tal, si nos ponemos a ver delitos informáticos típicos en Costa Rica, hay una sección del código penal que señala delitos informáticos y conexos, las reformas también han introducido la estafa informática que sin duda alguna ese si es un delito informático que se coloca en otra sección del código penal.

-Entonces creo que es un tema muy complicado la definición de ciber delito y hay muchísimas excepciones.

2) ¿Existe algún perfil de quien comete delitos informáticos?

-La perfilación dependerá mucho de la definición de lo que sea delito informático y del grado de participación que pueda tener esta persona sea un autor o un cómplice.

-En cuanto los autores se han dicho mucho, que suelen ser personas principalmente hombres que rondan entre los 12 o 15 años hasta los 40 o 50 años aproximadamente ya que se supone que después de los doce años ya se tiene intereses más versátiles y se empieza a integrar con este tema de las computadoras y se suele limitar por los 40 o 50 años por un tema de generacional, entonces se suele decir que no sean los más versados en la materia y se suele catalogar como las personas que hayan nacido por ahí de los años 70.

-Entre otros aspectos aparte de la edad pueden ser profesionales o estudiados ya que al autor se le suele catalogar como una persona inteligente que pueda manejar por encima del promedio todo el tema de la informática, computadoras, redes, que pueda entender cuál es el funcionamiento y cuáles son las potencialidades para eventualmente buscar las zonas oscuras para aprovecharse del sistema, se suele decir que es una persona auto motivada que muchas veces le gusta ponerse retos violar un sistema informático, la seguridad de un banco o algo por el estilo.

-El autor intelectual es una persona con muchísima habilidad llega y logra violentar un sistema bancario o estafar un montón de gente, hacen una página phishing para recolectar datos de personas, sabe cómo funciona todo y es el que menos se expone pero necesita hacer efectivo el dinero que recaudo, entonces ¿a quién pone? a los partícipes que son personas muy humildes que buscan oportunidades muy sencillas para ganar dinero, como el típico caso de préstame tu cuenta porque necesito que me transfieran un dinero, muchas veces estas personas saben que el dinero es sucio, les transfieren el dinero, van al banco, lo sacan y los partícipes son los que eventualmente terminan agarrando.

-También con una pequeña asesoría se elimina el dolo y se podría lograr la libertad, diciendo el participante que él no sabía nada, que le dijeron que era dinero limpio, que a mí me dijeron que me daban una comisión porque no tenía cuenta en el país para recibir el dinero, sin embargo, muchas de esas personas si sabían lo que estaban haciendo y que provenía de tema delictivo.

3) ¿Es difícil identificar a los sujetos activos de los delitos informáticos?

-Al autor intelectual, si es sumamente difícil, porque es el que esta atrás de todo, a veces nada más le llega el dinero y nadie sabe quién es este jefe ni donde vive, porque uno de los principales atributos es que son por excelencia internacionales por medio del internet una persona de China puede estar en este momento hackeando a alguien de Costa Rica o puede estar reclutando a participes para que se metan en ese esquema.

Entonces identificarlo si es muy complicado por no decir imposible, a los partícipes si es más fácil, que son los que al final terminan pagando los platos rotos.

4) ¿Cuál es el mayor problema judicialmente a la hora de afrontar un proceso judicial por este tipo de delitos?

-En todo el tema de investigación está la dificultad de identificar a los autores, de lograr pruebas, mucho de lo que está involucrado esta fuera del país como los servidores en Estados Unidos, Facebook, llamar a Google depender de la buena fe de hechos en el tema probatorio.

-Por lado del OIJ cuenta con recursos muy limitados tanto en materiales, como económicos y como recurso humano son sumamente capacitados sin embargo el delito informático cambia demasiado rápido.

-Desde la óptica procesal, hay bastante desconocimiento de los operadores jurídicos, tanto de la fiscalía, como también hay pocos defensores públicos que dominen el tema, los litigantes particulares tampoco lo dominan, incluso los señores jueces no dominan mucho el tema.

-***Debería haber una capacitación mayor sobre delitos informáticos e incluso especialización.***

-En el ámbito operacional en general el país cuenta con demasiados delitos y la falta de recursos no es precisamente en esta materia, la expansión de derecho penal es absurda y ahora cualquier conducta es delito, no hemos priorizado esa política criminal

5) Según su experiencia, para procesar penalmente a un delincuente informático ¿cuál ha sido su conocimiento?

-Dependerá de la persona que estamos sentando en el banquillo, si es el mulero que falsifico una tarjeta de crédito y lo agarraron en cámaras o hizo un dispositivo en el cajero automático para captar la banda magnética y luego alguna persona va y saca el dinero esa persona no suele ser tan complicado, ya que hay muchos videos de seguridad entonces no es tan complicado llevarlos a juicio.

-En cuanto los autores no he podido llegar a saber quién cometió el delito.

6) ¿La terminología del tipo penal, crea algún problema que se habla de phishing, hardware, software?

-La terminología suele utilizar muchos anglicismos, los que dominan el mundo de internet y la tecnología suelen ser los estadounidenses y los chinos, entonces si hay muchos anti sismos como *phishing, rooming* que es establecer contacto con personas menores de edad.

-Toda la terminología suele estar en inglés, hay traducciones, pero sin embargo pierden su significado entonces la gente lo utiliza generalmente en inglés.

7) ¿Con el tema de la estafa ha visto algún problema en el tipo penal especifico que a veces se utiliza el 2 16 otras el 2 17?

- el 2 16 es la estafa pura y simple.

- el 2 17 BIS es el de la estafa informática.

-Yo creo que los tribunales, se han inclinado por hacer la distinción tal y como la hace Francisco Castillo, de darle a la estafa donde aquel medio que se utiliza en fundamentalmente el sistema procesamiento automático de datos “la computadora”

-En cuanto dificultades en el tipo penal el articulo 2 17 BIS dice que la definición de ***“un dato es aquella pieza sin significado sin orden que eventualmente si lo sistematiza puede representar algo, este algo es lo que se conoce como información.”***

-Lo que ha pasado en la práctica, es que ha habido mucha dificultad para conocer esa distinción entre conocimiento de un dato, información ordenada, que no es un tema que este estrictamente en el tipo penal del 216 o 217 pero si hace dificultad que vale la pena mencionar.

-La dificultad principal estaría en la definición misma, ya que no sabemos claramente que es una estafa informática ya que queda tan amplio que ***todo delito calzaría mientras allá una***

computadora involucrada, si hay cierto orden de los operadores jurídicos de poder excluir un poco… ¿es o no es la computadora el medio fundamental?

8) ¿Deberían los estudiantes de derecho llevar una materia sobre delitos informáticos en la universidad?

- No sé si en lo personal lo incluiría como parte fundamental del currículo en las universidades, una opción sería aplicarlo como curso optativo o una rama de especialización dentro de la misma licenciatura, ya que si está incrementando, si lo incorporaría dentro los programas, no sé si dentro de la base ya que si hay un nivel muy alto de especialización para comprender el asunto, entonces tampoco vamos a extender el currículo de una carrera a una persona que no tenga el interés en derecho penal pero si incluiría dentro de todas las materias un poquito de la parte informática ya que no se maneja en lo más mínimo.

9) ¿Que recomendaciones daría para mejorar los procesamientos de delitos informáticos en Costa Rica?

- Capacitación sobre todo en las personas que están involucradas en este aspecto, la fiscalía, los defensores, los jueces.

-Mejoramiento de recurso humano, pero también recurso material, el OIJ necesita mejores equipos para poder eventualmente investigar ya que tienen muy pocos dispositivos para eventualmente respaldar los discos duros.

- Interés en la materia, ya que la gente le huye al tema tal vez por desconocimiento de la materia.

-Regulación típica, creo que si empezamos a crear tipos penales de una manera descontrolada y a cerrar el ámbito de la libertad nos convertiríamos en un país que no queremos, saber clasificar en lo que ya tenemos en el código.

-Unificar parece que está un poco desordenado, ya que todo eso es parte de la misma dificultad de definición, ¿cuál es el bien jurídico tutelado del homicidio de las lesiones? Claramente es la vida, ¿del robo y del hurto? Claro, pero en estafas informáticas tenemos tenencia y difusión de material pornográfico o de personas menores de edad ya que se comparte por computadoras, pero es eso realmente un delito informático.

-No sé si unificarlo sea prudente ya que en la aplicación práctica difícilmente haga alguna diferencia.

10) En el artículo 230 que es el de suplantación de identidad ¿ve algún problema con respecto a la terminología?

"Será sancionada con pena de prisión de uno a tres años a quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, medio electrónico o tecnológico de información."

-El problema que veo es que esto se da todos los días, ya que es de los delitos informáticos más comunes y menos perseguidos.

-Aquí en Costa Rica lo que hay es estafas informáticas, pero de cajero automático ese es el delito informático por excelencia, en donde el mulero va y saca el dinero del banco, pero la suplantación es el pan de cada día, la gente solamente lo denuncia en Facebook, Instagram que es el típico ayúdenme a denunciar perfil falso ósea confían más en lo que puede hacer una red que en lo que puede hacer una autoridad judicial.

-En el 236 que difusión de información falsa hay un tema de amplitud del tipo penal que es una noticia o hecho falso capaz de distorsionar o causar perjuicio de seguridad al sistema financiero y a sus usuarios, en este mundo donde cualquier cosa se vuelve viral podríamos decir que cualquier cosa sería capaz de eso, el tipo penal está pensado que sea un medio idóneo para

cometer el delito, pero de nuevo es el típico caso que se planteaba la doctrina que pasa si usted corta una persona con una hojita de papel sabiendo que no es capaz de producirle muerte sin embargo se le infecciona y se muera.

Cualquier cosa se vuelve viral y daña a cualquiera como sucedió con el BAC que experimento la difusión de la noticia que iba a quebrar y de la noche a la mañana las perdonas empezaron a sacar su dinero.

"El tipo se considera delito con solamente difundirlo."

Dirigido a abogados Litigantes, para identificar aportes vivenciales en el abordaje de los delitos informáticos en el marco jurídico costarricense, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente José Benjamin Hidalgo Durán, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Lic. Adalid Medrano Melara. Abogado litigante.

1) ¿Qué es un ciberdelito o delito informático?

-Un delito informático, es toda aquella acción delictiva informática, dirigida a vulnerar la confidencialidad, la integridad y la disponibilidad de los sistemas o datos informáticos o contra la autodeterminación informativa o identidad en medios electrónicos.

Esto sería una definición propia de qué es un delito informático, de acuerdo a la legislación de nuestro país, esto porque sí sólo definiéramos los delitos informáticos como aquellos que atentan contra la confidencialidad, integridad y disponibilidad, estaríamos dejando delitos importantes, como lo son la suplantación de identidad y la violación de datos personales, que técnicamente no requieren ni si quiera vulnerar la seguridad de un sistema informático para realizarlos, y tutelan otros bienes jurídicos de gran importancia para la sociedad moderna.

2) De conformidad con la pregunta anterior, ¿podría explicar algunos de los delitos informáticos?

-En el ámbito de las estafas informáticas, por medio del tipo penal, es bastante complejo, ya que tomando en cuenta que los delincuentes, los mueve el lucro, por supuesto, que cuando nos encontramos ante sistemas informáticos que gestionan patrimonio o dinero electrónico, los delincuentes van a querer buscar muchas formas de lograr, este tipo de beneficio patrimonial. En ese sentido, ***podemos decir que es uno de los delitos que más le afectan a los costarricenses a diario*** y que se comete a través de diversas conductas delictivas.

Entonces, cuando lo vemos así, podemos observar que la estafa informática, es de momento la que más afectación está generando a la población costarricense y donde diversos delitos informáticos se encuentran en el "*iter criminis*", lo que permite combatirlo antes de que se genere el perjuicio patrimonial.

En el camino hacia la comisión de la estafa informática, nos encontramos con delitos informáticos como **la suplantación de páginas electrónicas (artículo 233, Código Penal)**, el cual es un delito que se suplanta un sitio legítimo de internet como un banco, con el fin de engañar a los clientes, para que brinden información, que les va a servir para cometer la estafa informática que desean realizar. Los delincuentes ***suplantan un sitio legítimo en internet, en perjuicio de un tercero y existe un agravante si se utiliza para obtener datos confidenciales de una víctima****"*. Como le indiqué, en este caso nos encontraríamos con un delito que se encuentra definitivamente en el camino de la estafa informática (artículo 217 bis, Código Penal), ya que estos son unos de las rutas habituales que utilizan los delincuentes en este delito.

Por otro lado, también se encuentra la suplantación de identidad (Artículo 230, Código Penal), que normalmente se comete cuando los delincuentes envían correos electrónicos masivos, donde a las personas les hacen creer que están comunicándose con una entidad bancaria y a partir de ahí logran engañar a las personas, para que se dirijan a un sitio web suplantado (Artículo 233, Código Penal), para que instalen un programa informático malicioso (Artículo 232, Código Penal), que les permita a los delincuentes lograr las herramientas o caminos, para ingresar al sistema bancario nacional, en nombre del usuario legítimo (Artículo 230, Código Penal) y hacer transferencias ilegales, entonces podemos observar que también nos encontramos con otro delito que suele estar en el *"iter críminis*" de la estafa informática que es: "***La instalación o propagación***

de programas informáticos maliciosos" este delito se encuentra en el artículo: 232 del código penal, es un delito bastante complejo, tiene muchas acciones dentro de las que se encuentran:

- Instalar programas informáticos maliciosos.
- Engañar a una persona para que instale un programa informático malicioso.
- Convertir a una página electrónica legítima en un sitio malicioso atacante.

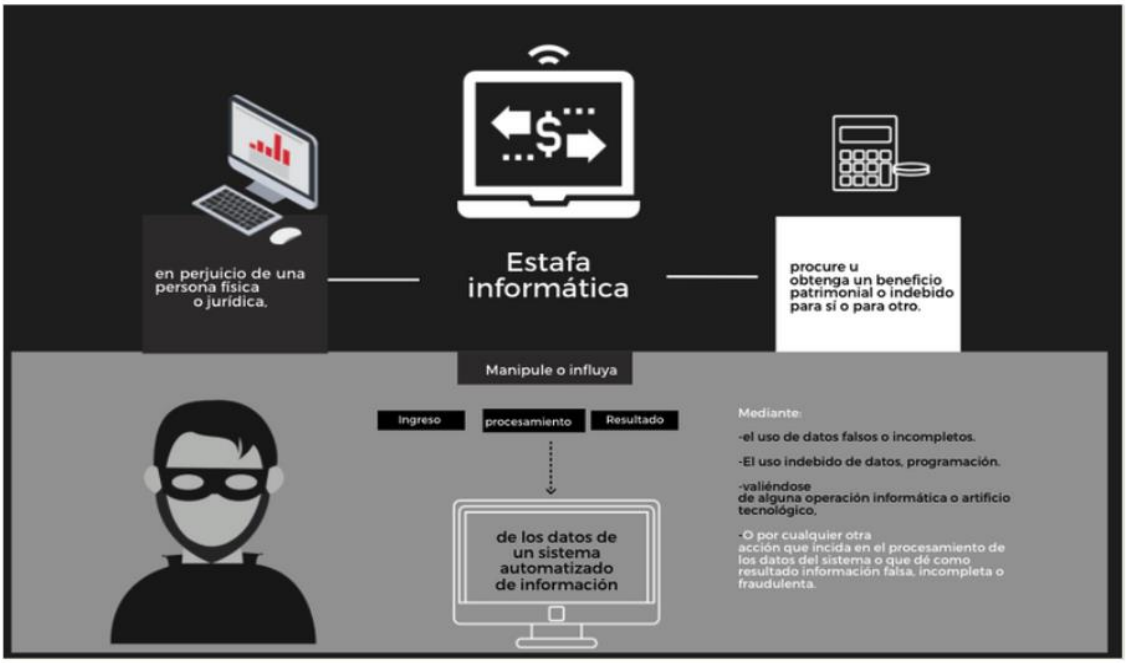
A través de los puntos anteriores, el delincuente logra abrir el camino para defraudar a las personas.

También nos encontramos la violación de datos personales (Artículo 196 bis, Código Penal), en el caso de Costa Rica, es una metodología utilizada muy frecuente, porque es el mercado negro de datos personales de los costarricenses, a través del cual los delincuentes hacen intercambio de bases de datos, para llamar a las personas y engañarles haciéndose pasar por entidades bancarias, le dan información que en principio solo debería tener su banco de confianza, las personas confían y pueden a partir de ahí ingresar a los sitios suplantados, pueden interactuar con una persona que se hace pasar por un funcionario bancario y hasta le pueden instalar el programa malicioso.

Finalmente, vamos a analizar otro delito, el cual les brinda los medios informáticos a los estafadores informáticos y es el delito facilitador del delito informático (artículo 234, Código Penal) y siendo una de las acciones más comunes el de personas que alquilan conscientemente, los servidores de páginas web y de correo electrónico a delincuentes, para que comentan acciones delictivas. Por ejemplo, ¿sabía usted que hay lugares que conociendo que los delincuentes, tienen necesidades informáticas les alquilan los servidores en forma de cripto-moneda para que los utilicen en lo que ellos quieran y de esta forma los delincuentes pueden tener múltiples páginas web, donde suplantan entidades bancarias, instituciones financiaras, para engañar a personas y así

propagar los programas informáticos que les ayuden en general para lograr este beneficio patrimonial? Entonces viéndolo de esa manera nos encontramos que antes de llegar al beneficio patrimonial, los maestros del engaño, que son los delincuentes informáticos, logran sin duda cometer distintos delitos informáticos.

Estructura del delito de estafa informática.



Fuente: www.adalidmedrano.com

-Se impondrá de prisión tres a seis años a quien en perjuicio de una persona física o jurídica manipule o influya en el ingreso, procesamiento o resultado de los datos de un sistema automatizado, ya sea mediante uso de datos falsos o incompletos, uso indebido de datos, en programación, está la norma indicando que hay una instalación de un programa informático malicioso.

Por supuesto que cuando se da la instalación de un programa informático malicioso, nos encontramos ante un concurso aparente de normas, siendo la instalación del programa informático malicioso necesaria para la estafa informática, valiéndose de alguna operación informática, artificio tecnológico o bien por cualquier otra acción que incida en el procesamiento de datos en el sistema, o que dé como resultado información falsa incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para un tercero, aquí es importante que usted tome en cuenta que este tipo penal se debe cometer en contra de una persona física o jurídica, normalmente se hace en contra de una persona física, que son los clientes del sistema financiero nacional, el delincuente influye en las tres fases que tiene todo sistema informático qué son: ***ingreso de datos, proceso los datos y el resultado de los mismos*** y a través de esta manipulación o influencia, por uso de datos falsos incompletos, que es lo que dice el tipo penal, el uso indebido de los mismos, programación y todos estos, procuran u obtenga un beneficio patrimonial indebido para sí o para un tercero, es de estos tipos penales, donde normalmente se da en el sistema financiero nacional y aquí es importante destacar que en el párrafo segundo que tiene que ver con el agravante del mismo del 267 BIS del Código Penal, en ese apartado viene un agravante, cuando se da contra sistema de información público, sistemas información bancaria o sistemas de entidades financieras, quiere decir que, cuando nos encontramos ante estafas informáticas, en su mayoría nos encontramos con una pena de prisión menor de 5 a 10 lo que quiere decir que en

nuestro país no importa si usted hace una transferencia ilegal de un monto insignificante igual la pena mínima es de 5 años, por supuesto que nos encontramos ante un error de legislador, por otro lado la estafa informática por su forma de haber sido construida como tipo penal, nos permite que sí sé da una estafa informática, digamos que por una cripto-moneda, no utilizando una entidad parte de un sistema financiero nacional, sino una red descentralizada que no está debidamente regulada, igual al tener contenido patrimonial una cripto-moneda se puede configurar la estafa informática.

Entonces si a usted le roban sus *bitcoins* - o cualquier otra cripto-moneda- nos encontramos ante un delito informático, por otro lado, podemos ver temas como envío de mensajes de texto a través de las redes de telecomunicaciones, cómo es: Sinpe Móvil donde cualquiera podría pensar que no le aplica la estafa informática: pero sí a usted le roban su celular y este celular le quitan el chip y a través de eso le suplantan su identidad para enviar una estafa informática, son mensajes de texto como vehículo para la transferencia de fondos de un teléfono a otro, pues también se configura la estafa informática, a través del ingreso de datos en el sistema bancario, usando los mensajes de texto.

Entonces, cómo podemos ver, la estafa informática es un tipo penal complejo, y uno de los más estudiados, sobre los que hay más sentencias condenatorias en el país, es un tipo penal que se encuentra en el ordenamiento jurídico desde año 2001, que ha sido reformado y digamos que ha sido mejorado en la reformas de los #9048 y #9135 de los años 2012-2013, de forma correspondiente y que sin duda aún pareciera que aún quedan elementos para mejorar, desde la perspectiva de la política criminal, porque no es posible que un tipo penal como el de la Estafa informático, tengo una pena mínima de 5 años cuando está involucrada una entidad financiera, porque la mayoría de estafas se dan contra estas y no importa si es un adolescente o una persona

joven de 18 años y se robó cien mil colones igual la pena mínima sea de cinco años, entonces este tipo penal, tal vez fue construido desde la perspectiva, de que los delitos informáticos son especializados, que se requiere muchos conocimientos por parte de las personas y por ende requiere penas mayores, pero está ampliamente demostrado que es un delito que no necesariamente requiere tanto conocimiento informático especializado por parte del actor para ejecutarse porque solo es necesario saber en algunos casos el usuario y la contraseña de una persona para cometer la estafa. O existen casos como el Banco Popular de Costa Rica, donde si usted tiene acceso al correo electrónico de la víctima, podría empezar el proceso de recuperación de contraseña y a partir de ahí tener acceso al sistema bancario, entonces, no podríamos decir que es un delito que requiere conocimientos especializados y que cualquiera puede ser un ciber delincuente.

3- ¿Cuál es el perfil de quien comete delitos informáticos?

-Cualquiera puede ser un ciberdelincuente, podríamos encontrarnos ante perfiles más especializados de lo que se llama esas personas que andan buscando de seguridad, que es el informático especializado, que logra crear herramientas que explotan vulnerabilidades, o sea, los caza vulnerabilidades, son personas de alto nivel informático y por otro lado vamos a tener las personas que simplemente utilizan herramientas generadas por otros, para cometerlos esto dentro de la comisión, que requiere algún tipo de herramienta especializada pero nos vamos a encontrar con delitos informáticos, en el ámbito casero o en el ámbito profesional donde lo único que se requiere es acceso al sistema informático privilegiado, sea usted informático, administrador o gerente, lo único que se ocupa es tener acceso y con dicho acceso cometer un delito informático Es importante que expliquemos que delitos como en revelación de correspondencia comunicaciones se requiere únicamente para cometerlo, el acceso a un documento privado y usted puede tener acceso a una computadora simplemente porque alguien la dejó desprotegida sin clave,

entonces no se requiere ningún conocimiento especializado para hacerlo, por ejemplo se requiere ningún conocimiento especializado si usted tiene acceso a una base de datos decide copiarla y venderla que se da el delito de violación de datos personales, entonces podemos decir que a diferencia lo que se hablaba hace muchos años donde se creía que el perfil del delincuente informático era muy especializado, ya nos encontramos ante una clase delitos donde cualquiera puede ser víctima pero cualquiera puede ser victimario también.

4- ¿Cuál es el perfil del sujeto pasivo?

-El perfil de un delito informático es muy amplio, cualquiera puede ser víctima, porque definitivamente nos encontramos en una materia donde, por ejemplo, usted en su casa trabajando o en sus dispositivos móviles en actividades privadas y alguien podría estar viendo sus comunicaciones.

¿Cuál es el perfil? Cualquier persona que use medios tecnológicos puede ser víctima o sujeto pasivo de un delito informático.

Si hablamos en el caso de estafa informática que es un delito informático específico con mayor alcance, nos encontramos que normalmente suelen ser personas con poco conocimiento de informática, porque de los timos de la forma de proceder más comunes de la ciberdelincuencia nacional es engañar a las personas por medio de ataque de ingeniería social por teléfono (vishing) y a partir de eso tener información, para engañarles y lograr obtener tener acceso al sistema bancario. Así que suelen ser personas con menores conocimientos en informática que probablemente esto sea un perfil que supera a más del 95% de la población costarricense, porque nadie en este país recibe desde la escuela, el colegio, la suficiente educación sobre seguridad informática y protocolos para protegerse de los cibercriminales, lo que hace que cualquier persona

costarricense de todos los rangos de edad, de todas las profesiones incluyendo las informáticas pueden ser víctimas.

5- ¿Se debería de crear en el currículum escolar o de colegio, alguna materia donde se eduque a la población sobre cómo protegerse de los delitos informáticos?

-Deberían enseñar elementos básicos de ciberseguridad en las escuelas, pero también tomemos en cuenta que ya hay personas que no van a pasar por la escuela, ni por el colegio, ni por la universidades y sino que son profesionales adultos que no han recibido nunca clases de ciberseguridad, que son activos dentro del sistema financiero nacional, dentro de las redes sociales, dentro de todo tipo de sistemas electrónicos, por lo tanto, es una población a las que se le promueven que utilicen las nuevas tecnologías con todos los procesos de transformación digital que tiene nuestra sociedad, pero que nadie les está enseñando sobre seguridad informática, entonces es algo que se tiene que enseñar de la misma forma que el higiene se enseña desde las escuelas y conforme van creciendo se van profundizando, este conocimiento pero también tomando en cuenta que somos una sociedad que apenas estamos empezando a romper la brecha digital, también tenemos que crear programas dirigidos a toda la población que sean integrales para tener conocimientos básicos para no solo utilizar plataformas de sistema financiero nacional sino también protegernos en nuestra vida cotidiana. Por ejemplo, el mero hecho de no configurar un segundo factor de autenticación en nuestros correos electrónicos o en nuestras cuentas de redes sociales puede hacer la diferencia entre ser víctima de un delito informático o no… ¿Por qué? Porque sabemos que las claves las contraseñas son una medida de seguridad obsoleta ante los ataques que se está dando en el presente ya que es muy común que se estén robando bases de datos con contraseñas de servicios digitales y a partir de ahí los clientes de estos sistemas informáticos o servicios informáticos son vulnerables ante los delincuentes que han tenido acceso a sus

contraseñas, imaginemos que nos roban la clave del Gmail que es su proveedor de correo electrónico, por lo tanto usted cree que está protegido porque tiene una clave de 50 dígitos y a partir de ahí el delincuente tiene acceso a su cuenta directa puede acceder a ella, lo que se acostumbra es que se tenga un segundo factor de autenticación que podría ser un elemento algo que conoce, algo que sabe, o algo que tenga en su posición y normalmente lo que se aconseja es que sea una aplicación que va generando los códigos de forma frecuente o una llave que solo usted tiene en su posesión y que le permite adicional a su contraseña probar que usted es quien dice ser.

Por otro lado, en Costa Rica nos encontramos con la firma digital certificada que puede dar seguridad en las transacciones bancarias. Debemos tomar en cuenta que la firma digital posee un gran valor para las personas por lo que no ha sido de amplio acceso, entonces tenemos a la población desprotegida, porque no le damos las herramientas necesarias ni les educamos cómo se debe.

6- ¿Cuáles son los delitos más comunes?

Entre los 5 más denunciados se encuentran:

1-La estafa informática.

2-Suplantación de identidad.

3-Difusión de información falsa.

4-La violación de correspondencia o comunicaciones.

5-La seducción o encuentro de menores por encuentros electrónicos.

7- ¿Es difícil identificar a los sujetos activos del delito informático?

Si, ya que al tener una ciberdelincuencia especializada cuenta con herramientas especializadas para no ser detectados, pero qué pasa cuando la ciberdelincuencia no es especializada y es casera, por ejemplo, usted decide ingresar a la cuenta electrónica de su ex esposa

desde su trabajo, empieza ingresar, detectan que hay unos accesos ilegales, su ex esposa pone la denuncia, se apersona al OIJ, entonces como ella tiene acceso a las propias estadísticas de su correo electrónico, pide el estudio de una fecha y hora específica que es donde se dio cuenta que ingresaron a su correo, con el fin que le indiquen el nombre del suscriptor entonces de una forma muy sencilla se podría vincular una persona con esto.

Podría ser que en la bitácora del "*router*" se note que usted no fue la persona que se conectó ya que se encontraba fuera de la casa sino algún familiar, pero ahí es donde viene el tema que estamos dejando tanto rastro por medio de medios electrónicos que la evidencia digital es esencial y en algunos casos logra facilitar vincular a una persona con alguna acción delictiva pero cuando nos encontramos con actores profesionales con mínimos conocimientos de informática podría ser muy difícil vinculare. ***Puede ser muy fácil cuando nos encontramos ante personas no especializadas y muy difícil cuando nos encontramos con personas de alto conocimiento.***

8- ¿Cuál es el mayor problema a la hora de enfrentar un proceso judicial por delitos informáticos?

-Tenemos que tomar en cuenta que los retos son múltiples, tenemos la primera que vamos a encontrar y se lo voy a decir por etapas la primera sería al momento de poner la denuncia, no hay personal capacitado sobre este tipo de materia, como mencionamos anteriormente entre los delitos que aparecen de primero está difusión de información falsa que sólo hay un caso conocido de este tipo penal, que es difundir información falsa, capaz de afectar el sistema financiero nacional, es un tipo penal que viene a proteger al sistema financiero nacional de noticias, como las que dicen que va a quebrar tal banco o tal otro y que la gente empieza a sacar sus fondos, por ejemplo, en casos como éste son muy poco frecuentes, pero cómo es posible que sólo el año pasado se anunciaran 87 de esos, pareciera poco probable, que un hecho como eso, con la capacidad de

afectar al sistema financiero nacional no haya salido ni en medios, nos encontramos entonces ante denuncias que están mal calificadas por el receptor, por lo tanto eso hace que cuando llegué al investigador especializado que lo va a ver, también nos encontremos contra otro reto porque al haber desconocimiento de los investigadores, puede ser que de una forma muy fácil están archivando estos casos, entonces por otro lado nos vamos a enfrentar ya desde una perspectiva más compleja con que a la hora de nosotros investigar un delito informático de carácter transnacional, nos vamos a enfrentar con las murallas de la falta de cooperación de grandes empresas tecnológicas, igualmente, falta de cooperación de altos niveles de solicitudes de naciones como la estadounidense y al mismo tiempo nos vamos a encontrar a una persona con una dirección IP que cuando la obtenemos los proveedores nacionales duran bastante tiempo para entregar la información a las autoridades, es por esto que a través del proyecto de ley 21 187 se trata de proponer la reducción de los tiempos de entrega de la información por parte de los proveedores de internet, de la información requerida en las investigaciones, entonces también nos vamos a enfrentar con el desconocimiento por parte de Fiscales en la materia, por lo que podría llegar a desestimar a las personas porque a falta de conocimientos, no logran obtener suficiente información, no cuentan en las herramientas tecnológicas o el conocimiento para detectar los casos, entonces va a ser otra barrera y como todo la evidencia digital representa un reto a nivel nacional.

9- Según su experiencia en caso de existir problemas ¿Cuáles son los principales impedimentos u obstáculos para poder procesar penalmente a los delincuentes informáticos?

Nos encontramos ante un problema de carácter probatorio y es que digamos que la fiscalía o el querellante, pueda generar suficiente elenco probatorio para poder vincular a una persona con un hecho sin que quede el espacio para la duda.

El problema es que para que logremos tener esto, tiene que haber suficiente conocimiento en la materia por parte de Fiscales y Jueces para poder determinar que una prueba puede ser suficiente o no y entonces es la complejidad de la evidencia digital, que tenga la suficiente fuerza probatoria, que las personas no presenten simplemente pantallazos de algo que pasó porque un pantallazo es altamente manipulable se puede poner su cara en cualquier lugar entonces por supuesto que las personas cuando entregan la prueba tienen q hacerlo de manera correcta en la etapa inicial del proceso donde se está recopilando la información entonces se nos presentan retos en esta materia para que los procesos avancen porque nos encontramos ante retos para la cooperación internacional, porque finalmente hay errores en el proceso vinculados con esta materia, es por esto que estos casos requieren un estudio mayor por parte de los litigantes y funcionarios.

10- Considera usted que los abogados deberían especializarse o al menos las universidades deberían de tener una materia específica sobre los delitos informáticos.

Estoy convencido que sí, de hecho, no solo los delitos informáticos, deberían tener el derecho informático como una materia que se debe dar, ojalá en uno o dos cursos para que los estudiantes puedan comprender bien esta materia y le explico por ejemplo yo ahorita estoy dando clases derecho informático en la Universidad Libre de Derecho entonces vemos tema de datos personales, comercio electrónico, delitos informáticos, firma digital entre otros temas importantes y sinceramente el cuatrimestre se hace insuficiente para la cantidad de información que deben conocer los profesionales del mañana, entonces es complicado, porque son pocas las universidades que dan en la clase derecho informático y en derecho penal hay muy pocos penalistas que estén manejando los delitos informáticos como tal, quiere decir que es un gran reto para las nuevas generaciones que se están incrementando los delitos informáticos, que son parte de nuestra vida

diaria y hay muchas personas que se encuentran en nuestro círculo familiar, empresarial y de amistades que pueden cometer delitos informáticos de una manera muy sencilla contra nosotros pero los profesionales ya sea en casos de familia, casos penales, que ven inclusive temas tributarios, porque sin duda el derecho informático es transversal y no se encuentran capacitados sobre esto, entonces por supuesto que se requiera a nivel nacional mucho mayor capacitación, mucho mayor esfuerzo, en ese sentido el Colegio de Abogados y Abogadas está haciendo grandes esfuerzos a través de comisiones como la de derecho informático, está iniciando una que se llama Innovación Regulatoria que va a analizar todos estos temas, porque es una necesidad que tenemos como país.

11- ¿Qué es necesario mejorar a nivel de la persecución de delitos informáticos?

Inicialmente, cuando se hace una propuesta de reforma del código penal, se requiera hacer un estudio de cuáles son las tendencias del cibercrimen y con base en eso debe generar una nueva política criminal, para combatirlos en ese sentido hay un proyecto de ley 21 187 que viene a mejorar temas como la creación por ejemplo de una estrategia de lucha contra el cibercrimen por parte del poder judicial, se viene crear un proceso mejores en la cooperación con las empresas nacionales e internacionales en la lucha contra el cibercrimen se incorporan nuevos tipos penales que vienen a ayudar en acciones que vienen en incremento como es el acoso cibernético, cómo es la suplantación de llaves de carros y con la utilización bulto con el cual pueden hacer uso a través de ciertos dispositivos y de esta manera darle a las autoridades mayores herramientas para luchar contra este nuevo flagelo que está enfrentando la sociedad, ahora es importante que las críticas que ha tenido no se incorpora ninguna fuente financiamiento para poder luchar contra el cibercrimen y por supuesto es una falencia que tiene muchos proyectos a nivel nacional, sin embargo, este proyecto se inició como una discusión en donde los diputados deben de decidir de qué forma se

puede financiar la lucha contra el cibercrimen que nos afecta a todos y que por ejemplo en el Poder Judicial recientemente este año se creó una sección contra el cibercrimen dentro de la fiscalía segunda llamada fiscalía adjunta de fraudes y cibercrimen y que en la actualidad tienen más de mil casos muchos de ellos son de estafas informáticas y sólo tienen dos Fiscales entonces sin duda con o sin reforma, requerimos que se le dé mayor presupuesto a lo que son la sección especializada contra el cibercrimen del OIJ y a la fiscalía ante adjunta de fraudes y cibercrimen porque los delitos informáticos se van incrementando y pareciera que las autoridades no tienen ni una estrategia de capacitación ni una estrategia de lucha contra el ciber crimen, por lo que los delincuentes nos van a llevar la gran ventaja y no hay orden en la casa.

12) Según su conocimiento, ¡los problemas de seguridad informática, han hecho cambiar en la población, la forma en la que utiliza las redes sociales o el internet?

Es una muy buena pregunta porque si bien es cierto han habido delitos informáticos principalmente las estafas informáticas parte de la agenda de discusión nacional a través de diferentes reportajes como los artículos de prensa e inclusive notas informativas idiomas, espacios pagados este fenómeno no es suficiente porque la ciberdelincuencia es organizada y no hay sector de la delincuencia que cambie tan rápido y se adapte a los nuevos retos mientras la gente empieza a aprender que no tienen que dar datos por teléfono, los delincuentes ya lo saben le dicen que no le van a pedir datos, los envían a una página suplantada, la persona cree que está en el sitio oficial y empiezan a poner todos los datos y en el futuro nos enfrentaremos a lo que ya están enfrentando otros países con programas informáticos maliciosos dirigidos al sector bancario que ya a usted lo pueden afectar no porque le llamen para pedirle datos sobre su entidad bancaria sino porque le van a ofrecer una aplicación muy llamativa y estos datos que van a ser utilizados por este programa

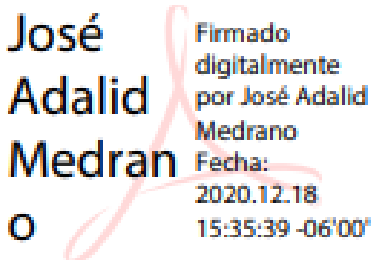
malicioso van a ser vendidos y van a ser utilizados por el cibercrimen local lo cual va a generar que los costarricenses no podamos luchar contra esto.

Si a los clientes del sistema nacional los están estafando, cuando la protección depende de que ellos no den datos, que pasaría cuando las estafas se cometan por medio de programas informáticos maliciosos donde los clientes del todo no tienen forma de protegerse, sino es a favor de la educación, eso va a ser todavía más grave, entonces no importa cuántas campañas de concientización se hagan sobre la materia, cuantos reportajes o noticias se den sobre el cibercrimen, la única forma que tienen las personas de combatir contra ese fenómeno es a través de un aprendizaje mucho más profundo, deben llevar cursos, informarse más, hacer más conciencia. ***La ciberdelincuencia mejora con mucha más rapidez y los ciudadanos deben capacitarse con igual celeridad o quedan en indefensión.***

Consentimiento informado Lic. Adalid Medrano Melara. Abogado litigante.

CONSENTIMIENTO INFORMADO

Yo, José Adalid Medrano Melara, con cédula de identidad número 800740684, autorizó la captura de mi voz para fines de transcribir la entrevista brindada, se utilice el texto obtenido de esta y se referencie mi nombre para efectos de la investigación, la cual es: LA ESPECIFICIDAD DE CONOCIMIENTOS EN LOS DELITOS INFORMÁTICOS del estudiante: JOSÉ BENJAMIN HIDALGO DURAN, cédula de identidad número: 205050745, de la Maestría de Derecho Penal, de la Universidad Internacional de las Américas (UIA). De la misma manera, autorizo la utilización de las imágenes aportadas durante la entrevista para ser utilizadas exclusivamente en dicho trabajo y presentación. ES TODO.



Dirigido a ingenieros informáticos, para identificar aportes vivenciales en el abordaje de los delitos informáticos desde el punto de vista de los especialistas en el área tecnológica, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente **José Benjamin Hidalgo Durán**, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Ing. Luis Diego Alfaro Alpízar. Ingeniero en informática.

1. **¿Qué es un ciberdelito o delito informático?**

Acción o acciones que se realizan a través de medios electrónicos o se involucre medios electrónicos para objetivos como distorsión, usurpación, robo entre otros por los cuales una persona puede tener una afectación directa en su integridad física o emocional, que puedan causar efectos y/o consecuencias en el momento o en el futuro.

2. **¿Existe algún perfil del delincuente informático?**

En general no, pero evidentemente debe ser persona con conocimiento en el área informática o al menos poder aprender con facilidad. En algún tiempo si se hacía un perfil y se señalaba a la persona estudiosa del área que se mantenía callada o muy involucrada siempre en la computadora. Sin embargo, es digno de comentar que en esta área hay definidos tres líneas específicas que se llaman sombreros: Blanco: los que ayudan; negro, los que afectan; gris, los que no están ni a favor ni en contra y muchas veces no definen en que parte se encuentran, puesto que pueden estar en las dos. Ahora no hay que dejar de lado que a lo largo de la historia siempre se decía hacker de forma malintencionada, aunque esto ha cambiado porque se incluyó como hacker ético parte de las personas que ayudan.

3. **¿Por qué es tan difícil perseguir delitos informáticos?**

Porque las personas que trabajan dañando o generando el delito, en la mayoría de los casos se enmascaran para ser indetectables, además que hay tanto desconocimiento del área que no logran llegar al origen del problema.

Otro detalle es que no se toman en cuenta desde el punto de vista del usuario muchas recomendaciones, y, por lo tanto, por más seguridad que se genere si el usuario final no aporta para mejorar, es muy difícil para los especialistas en el área poder lograr dar con la persona que comete el delito.

4. ¿Cuáles son los delitos informáticos más frecuentes que cometen los delincuentes en Costa Rica?

Probablemente sean las estafas, porque son las que se proceden a demandar o generar procesos de investigación en los entes judiciales. Pero en mi opinión diría que ronda más en distorsiones por robo de información, por encriptado de datos, pero muchas personas no lo denuncian por lo cual la estadística es complicada.

Además, el indicar que se sufre un ataque es exponer a las personas, instituciones y otros entes ante el escrutinio de una sociedad que aún no comprende que vivimos en el mundo digital y que como tal el mundo físico ya existe igual o más delitos que deben ser penados y/o multados.

5. ¿Es difícil identificar a los sujetos activos de delitos informáticos?

En algunas ocasiones, pero ahí es donde la informática forense ha ido trabajando para cambiar el día a día. Además de que la parte técnica ha pasado por un proceso de aprendizaje donde se le ha enseñado que todo debe ser trazable o rastreable con respecto a lo que se realizan en el día a día, pero no hay que dejar de lado que esto comienza a generar altos volúmenes de información y por lo tanto el proceso de identificar se comienza a complicar.

Ahora se trabaja de la mano porque sean los mismos algoritmos los que identifiquen este tipo de sujetos, pero apenas se está iniciando en muchos países como Costa Rica, sin embargo, hay países que han trabajado aún como lo es el caso de Israel, España, Estados Unidos creando unidades especializadas para la detección de este tipo de personas.

En la seguridad informática se trabaja en dos líneas ya establecidas: 1. La detección de ataques, la 2 La solución por ataques 3 es el ataque por lo que se generan protocolos para atender el antes, durante y después del ataque.

6. ¿Considera usted que las universidades deberían tener dentro de la carrera de derecho la materia de delitos informáticos?

Si, lo que pasa es que creo que aparte de delitos informáticos como materia, debe incluirse la parte de informática, pues son materias que separadas no funcionan tan bien cuando se debe ver específicamente este tema.

Entonces considerando lo anterior, sería difícil entender delitos informáticos sin al menos conocer de forma básica, y hasta en algunos de forma avanzada la parte informática. Se ha dicho por mucho tiempo que “cada uno es especialista en su área” pero esto para leyes debe cambiar; como lo hizo para informática desde el punto de vista de la incursión de otras materias no propias, por ejemplo: un informático que desarrolla o ver proyecto en el área financiera conoce de Contabilidad, finanzas e Incluso procesos propios del negocio y por lo tanto, las universidad se han renovado con acreditaciones que les permite cambiar sus planes de estudio para considerar en la enseñanza una diversidad de áreas con las cuales el profesional se topara cuando este en el ambiente laboral.

7. ¿Es difícil identificar a los delincuentes informáticos?

No, pero requiere técnica, experiencia y análisis de comportamientos que generar líneas de sospechas como se ha trabajado actualmente en su detección donde se involucra cuáles y como son los patrones para detección, podría decirse por ejemplo: si de una misma computadora se realizan constantes consultas sobre una entidad bancaria y este computador no pertenece al banco,

esto puede generar sospechas que pueden concretar en un delincuente, pero se trabaja en poder formar más especialistas en el área que den así con estos casos.

Dirigido a ingenieros informáticos, para identificar aportes vivenciales en el abordaje de los delitos informáticos desde el punto de vista de los especialistas en el área tecnológica, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente **José Benjamin Hidalgo Durán**, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Ing. Marisol Núñez Vásquez. Ingeniera en Informática.

1. ¿Qué es un ciberdelito o delito informático?

Cualquier acción o actividad ilegal que se realiza haciendo uso de la tecnología.

2. ¿Existe algún perfil del delincuente informático?

Puede ser cualquier persona con habilidad para el manejo de sistemas informáticos o que sus tareas laborales le facilitan el acceso de información de carácter sensible, puede ser desde un chico viviendo la experiencia de introducirse en equipos de acceso restringido solo por la emoción, hasta grupos organizados en el delito con distintos fines.

3. ¿Por qué es tan difícil perseguir delitos informáticos?

Se presentan varias características de los delitos informáticos que dificultan el tratarlos adecuadamente tales como:

Porque las huellas digitales, que pueden permitir la identificación de los culpables son difíciles de rastrear y se requieren recursos especializados.

El ejecutar un delito informático es muy rápido o se da casi de forma instantánea, se realizan en el ciberespacio por lo que es difícil aplicar la ley y más si se toma en cuenta que es difícil rastrear desde que lugar geográfico se realiza.

Cambian constantemente al ritmo que cambian las tecnologías haciendo difícil el definir los patrones de conducta.

4. ¿Cuáles son los delitos informáticos que más frecuentemente cometen los delincuentes en Costa Rica?

Según estadísticas del Organismo de Investigación Judicial los delitos más cometidos en Costa Rica son: la estafa informática, suplantación de identidad, difusión de información falsa, espionaje informático, seducción o encuentro con menores por medios electrónicos y en menos grado la facilitación del delito informático, instalación de programas maliciosos, suplantación de páginas electrónicas, sabotaje informático y daño a equipos. Sin omitir que se han presentado nuevas formas de delinquir que no se encuentran reguladas en nuestra legislación.

En mi perspectiva, muchos delitos no se reportan, son cometidos desde adentro de las organizaciones y no se reportan para evitar escándalo y pérdida de imagen.

5. ¿Es difícil identificar a los sujetos activos de delitos informáticos?

Considero que es difícil debido a que se requiere personal altamente calificado y actualmente en Costa Rica no se cuenta con carreras que especialicen en materia de delitos informáticos, informática forense que es diferente a Seguridad Informática. En otros países, el Colegio de Profesionales en Informática o su igual, cuentan con un cuerpo de peritos informáticos preparados y certificados, en nuestro país no. Luego existe un desligue entre el profesional de ámbito legal y el de ámbito informático que deben trabajar en conjunto y hablar un mismo idioma en delitos informáticos. Si no se trabaja en estrechar estas brechas, difícilmente tendremos los recursos para identificar y aplicar justicia a los delincuentes informáticos.

6. ¿Considera usted que las universidades deberían tener dentro de la carrera de derecho la materia de delitos informáticos?

Considero que esta modificación de currículo de la carrera de derecho nos está llegando tarde, y con un gran agravante en la medida que un profesional en derecho no entienda el delito informático no será posible penalizar al individuo que lo comete.

Considero que debe incluirse cuanto antes la especialidad de Derecho los conocimientos no solo del delito informático sino la preparación de todo el personal forense e investigador que se requiere para poder aplicar la ley.

7. ¿El difícil identificar a los delincuentes informáticos?

En la medida que no contemos con profesionales especializados será difícil crear los perfiles e identificar los patrones de conducta. Considero que es más difícil que identificar otro tipo de delincuentes, sin embargo, nuestra desventaja es carecer de los recursos necesarios y estar conscientes de que este tipo de delito es particular por los medios utilizados.

Consentimiento informado Ing. Marisol Núñez Vásquez. Ingeniera en Informática

CONSENTIMIENTO INFORMADO

Yo MARISOL NÚÑEZ VÁSQUEZ, con cédula de identidad número: 502590508, autorizó que se ponga mi nombre, que se grave mi voz, para efectos de la investigación, la cual es: LA ESPECIFICIDAD DE CONOCIMIENTOS EN LOS DELITOS INFORMÁTICOS, del estudiante: JOSE BENJAMIN HIDALGO DURAN, cedula de identidad número: 205050745, de la Maestría de Derecho Penal, de la Universidad Internacional de las Américas (UIA). Es Todo, firmo en San José a las 10:00 horas del día 26 del mes de Diciembre de 2020.

MARISOL NUÑEZ VASQUEZ (FIRMA)

Firmado digitalmente por MARISOL NUÑEZ VASQUEZ (FIRMA)
Fecha: 2020.12.26 22:23:55 -06'00'

FIRMA Digital.

Dirigido a jueces, para identificar aportes vivenciales en el abordaje de los delitos informáticos en el marco jurídico costarricense, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente José Benjamin Hidalgo Durán, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Lic. Olivier Ramírez Valverde. Juez de la República.

2. **¿Qué es un ciberdelito o delito informático?**

Son los ilícitos cometidos mediante el uso de mecanismos electrónicos o informáticos, los cuales se realizan en contra de personas comunes o entidades financieras, los cuales pueden vulnerar el patrimonio de algún ciudadano o vulnerar la intimidad del mismo

3. **¿Qué ley regula los delitos informáticos en Costa Rica?**

Los delitos informáticos están regulados en el Código Penal, encontramos el delito de violación de datos personales, estafa informática, alteración de datos o sabotaje electrónico y violación de comunicaciones electrónicas. De los anterior, es común escuchar la gran cantidad de denuncias por estafas informáticas

4. **¿Quién comete delitos informáticos?**

Cualquier persona puede cometer delitos informáticos.

5. **¿Quién es el sujeto pasivo en los delitos informáticos?**

Puede ser cualquier persona o entidad financiera.

6. **Según su experiencia. ¿Cuáles son los delitos informáticos más frecuentes que cometen los delincuentes?**

El delito informático más frecuente es la Estafa Informática. Mediante engaño sacan el dinero de las personas de sus cuentas bancarias, haciéndose pasar por personeros de entidades financieras o de otras entidades públicas y privadas, utilizando a la propia víctima como instrumento del delito.

7. **¿Es difícil identificar a los sujetos activos de delitos informáticos?**

Sí, es muy difícil identificar al sujeto activo, lo difícil es determinar quién es la persona que ha efectuado el ilícito a través de medios electrónicos. En la mayoría de casos la Policía Judicial, no tiene elementos probatorios para determinar quién es la persona que está efectuando el ardid o haciendo actos encaminados a la comisión delictiva, obteniendo dinero o información sensible de la víctima.

8. **¿Cuál es el mayor problema a la hora de enfrentar un proceso Judicial por delitos informáticos?**

El mayor problema es identificar al sujeto activo y también es un problema recuperar el dinero sustraído, dado que los delincuentes proceden rápidamente a la sustracción del dinero o moverlo de entidad financiera, volviéndose sumamente difícil recuperar el dinero.

9. **Según su experiencia, en caso de existir problemas. ¿Cuáles son los principales impedimentos u obstáculos para poder procesar penalmente a los delincuentes informáticos?**

El impedimento para procesar a los delincuentes es que dicho ilícito se puede cometer en cualquier parte del mundo, dificultando la ubicación del sujeto activo del ilícito y sobre todo determinar la identificación del delincuente.

10. **¿Considera usted que las universidades deberían incluir la materia de delitos informáticos?**

Claro, se debe incluir la materia de delitos informáticos, y el análisis del tipo, hay que recordar que el gran problema de los delitos informáticos es probatorio, grandes cantidades de expedientes son desestimados por falta de prueba; y por otro lado quienes denuncian ante el Ministerio Público pierden la fe y esperanza de recuperar su dinero, muchas veces por la lentitud nuestro sistema judicial.

11. **Con respecto al tema de los ciberdelitos y el procedimiento penal en Costa Rica. ¿Qué recomendaciones consideraría para mejorarlo?**

El Ministerio Público no tienen un tiempo de respuesta efectivo en sus primeras diligencias, por ejemplo, no solicitan el levantamiento del secreto bancario o tardan en hacerlo, tampoco solicitan al ofendido que presenten las pruebas, en este tipo de delitos como lo serían los estados de cuenta de la entidad financiera. El Ministerio Publico debe ser más efectivo a la hora de iniciar con las diligencias.

12. **¿Según su conocimiento los problemas de seguridad han hecho cambiar en la población la forma en que se utiliza el internet?**

La población en su gran mayoría ha sido más precavida a la hora de utilizar las herramientas electrónicas e internet, así como no brindar datos y no escribir datos en páginas extrañas o en llamada telefónicas, sin embargo, muchas personas aún siguen cayendo en los engaños. Por ejemplo, los delincuentes utilizan un *Software* con el cual aparece el número de teléfono de la entidad financiera de la cual suponen llamar, la persona al ver el número que es muy conocido piensa que me están llamando del Banco y en realidad no es así. Si se va mejorando, pero falta mucho, la delincuencia informática va a seguir lastimosamente.

Consentimiento informado. Lic. Olivier Ramírez Valverde. Juez de la República.

CONSENTIMIENTO INFORMADO

Yo Oliver Ramírez Valverde, con cédula de identidad número: 1-1343-0098, autorizó que se ponga mi nombre, que se grave mi voz, para efectos de la investigación, la cual es: LA ESPECIFICIDAD DE CONOCIMIENTOS EN LOS DELITOS INFORMÁTICOS, del estudiante: JOSE BENJAMIN HIDALGO DURAN, cedula de identidad número: 205050745, de la Maestría de Derecho Penal, de la Universidad Internacional de las Américas (UIA). Es Todo, firmo en Guápiles a las 10:00 horas del día 20 del mes de Diciembre de 2020.

Dirigido a jueces, para identificar aportes vivenciales en el abordaje de los delitos informáticos en el marco jurídico costarricense, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente José Benjamín Hidalgo Durán, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Lic. Erick Roberto Barrios Sancho. Juez de la República.

1.- Qué es un ciberdelito o delito informático?

Son los tipos penales que regulan las conductas delictivas cometidas por medio o con ocasión de medios y herramientas tecnológicas, tales como sistemas y equipos informáticos, electrónicos, bases de datos, teléfonos inteligentes, correos electrónicos, redes sociales y otros de simular naturaleza, tendientes en la mayoría de los casos a comprometer y afectar el patrimonio ajeno, sustraer información sensible de los derecho habientes (titular del derecho) y/o vulnerar el honor o la reputación de las personas físicas o jurídicas, para lo cual se procede a alterar, dañar, alterar o modificar los diversos sistemas electrónicos con el dichos

2.- Que ley regula los delitos informáticos en Costa Rica?

El Código Penal en sus numerales 217 bis, 229 bis, 229 ter, 230, 231, 232, 233 y 234 regula lo relativo a estos delitos, los cuales suelen cometerse en asocio con otros delitos como estafas, delitos contra el honor, como por ejemplo ofender la dignidad de una persona alterando una red social, etcétera. Los principales son la estafa informática, el daño informático, el sabotaje informático, la suplantación de identidad, el espionaje informático, la instalación o propagación de programas informáticos maliciosos, la suplantación de páginas electrónicas y la facilitación de delito informática entre los más comunes.

3.- Quién comete delitos informáticos?

Comete este delito cualquier persona física que dolosamente altere, suprima, dañe, modifique algún sistema electrónico, informático, telemático, red social u otro similar, y con ello genera algún perjuicio a los bienes jurídicos de una persona física o jurídica.

4.- Quién es el sujeto pasivo en los delitos informáticos?

Puede ser cualquier persona física o jurídica que sufra un daño, perjuicio o menoscabo patrimonial o en su honor con ocasión de la alteración, daño, modificación, sabotaje o irrupción ilegal de los datos o sistemas que pertenezcan a esa persona física o la empresa. Desde el punto de vista práctico, las víctimas más comunes de estos hechos delictivos son las personas físicas o empresas que tienen grandes sumas de dinero en cuentas de ahorro, corrientes, valores u otros, y que, mediante la alteración de datos o sistemas informáticos, los delincuentes sustraen claves o las descifran de modo ilegal o clandestino y sustraen los recursos económicos de estas personas. También se cometen delitos patrimoniales mediante la estafa electrónica en perjuicio de entidades bancarias y financieras, alterando y vulnerando la seguridad de la información, con el empleo de hackers informáticos. De ahí la importancia de que las empresas ejecuten controles y fiscalización diaria sobre las transacciones virtuales, manteniendo actualizados los sistemas de Tecnología de información y auditoría de los sistemas.

5.- Según su experiencia, ¿cuáles son los delitos informáticos más frecuentes que cometen los delincuentes?

Los más frecuentes son la estafa informática en perjuicio de bancos, personas físicas que manejan grandes sumas de dinero, y que por descuido facilitan los datos a los delincuentes quienes tienen acceso a sus cuentas, o bien mediante la utilización de hackers o piratas informáticos para vulnerar la seguridad de las empresas financieras. También son frecuentes los delitos contra el honor de las personas físicas y jurídicas, mediante publicación de ofensas e información falsa en las redes

sociales, como Facebook, WhatsApp e in line y otras similares. Recientemente han proliferado los delitos sexuales y la trata de personas utilizando el ciber espacio, lo que viene a denigrar a las personas, niños, niñas, mujeres y personas más vulnerables.

6.- Es difícil identificar a los sujetos activos de delito informáticos?

Precisamente como estos delitos se dan mediante la alteración de sistemas de información y electrónicos, es muy difícil dar al traste con los delincuentes que están detrás de tal ilícito negocio, ya que pueden estar en cualquier lugar del mundo o bien escondidos mediante algún perfil falso. Otro elemento que dificulta la investigación de los delitos informáticos es la falta de capacitación de los especialistas en el tema por parte de las autoridades, máxime que muchos de esos estafadores son delincuentes de cuello blanco, de alto nivel ligados al crimen organizado y desde luego puede contratar los mejores abogados, generando altos niveles de impunidad.

7.- Cuál es el mayor problema a la hora de enfrentar un proceso judicial por delitos informáticos?

El problema principal es la falta de recursos para especialización en la materia, fiscales especializados e investigadores del OIJ bien formados en la materia, lo que muchas veces perjudica el resultado de un proceso judicial, por falta de pruebas técnicas o una mayor investigación. Y recuerde que todo proceso penal se gana con pruebas, por el principio de carga de la prueba, sea el que acusa debe probar, por cuanto la duda favorece al encartado.

8.- Según su experiencia, en caso de existir problemas, ¿cuáles son los principales impedimentos u obstáculos para poder procesar penalmente a los delincuentes informáticos?

Para enumerar los principales, son la identificación de los culpables, la falta de prueba técnica, la falta de recursos financieros para capacitación e investigación, la falta de conocimientos especializados por parte de los entes acusadores y excesivo formalismo del proceso penal, que

muchas veces impide por ejemplo levantar el secreto bancario en forma ágil y efectiva, con lo cual se genera impunidad.

9.- Considera usted que las universidades deberían incluir en la materia de delitos informáticos?

En los tiempos que corren es imprescindible que los alumnos de derecho se especialicen en estos delitos, puesto que están de la mano con la tecnología y van mutando a medida que se desarrollan nuevos sistemas, la formación académica es una herramienta fundamental en esta materia.

10.- Con respecto al tema de los ciberdelitos y el procedimiento penal en Costa Rica, ¿qué recomendaciones consideraría para mejorarlo?

Modificaría la ley procesal penal para agilizar los trámites de levantamiento de secreto bancario y otras gestiones procesales para no depender de la orden del juez, sino que la fiscalía y el Organismo de Investigación Judicial tengan la facultad de pedir la información de manera más oportuna, además acortaría los plazos de resolución tratándose de la investigación de delitos informáticos para evitar impunidad por la lentitud de los procesos penales, es necesaria una jurisdicción especializada, como la jurisdicción penal de hacienda, para darle celeridad a estos procesos, puesto que los delincuentes informáticos actúan rápido, por lo que el proceso debe ir de la mano con la naturaleza de estos delitos.

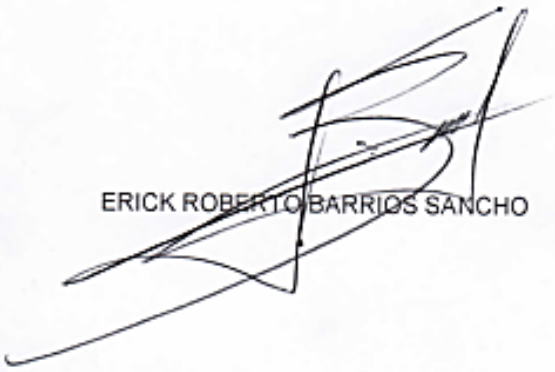
11.- Según su conocimiento los problemas de seguridad han hecho cambiar en la población la forma en que se utiliza el internet?

Me parece que aun la gente es muy confiada, y sigue dando sus claves de acceso de sus tarjetas y cuentas bancarias a desconocidos y las personas publican fotos y revelan datos personalísimos mediante las redes sociales, lo que propicia la comisión de estos delitos en forma creciente.

Consentimiento informado. Lic. Erick Roberto Barrios Sancho. Juez de la República.

CONSENTIMIENTO INFORMADO

Yo ERICK ROBERTO BARRIOS SANCHO**, con cédula de identidad número:** 204880468**, autorizó que se ponga mi nombre, que se grave mi voz, para efectos de la investigación, la cual es: LA ESPECIFICIDAD DE CONOCIMIENTOS EN LOS DELITOS INFORMÁTICOS, del estudiante: JOSE BENJAMIN HIDALGO DURAN, cedula de identidad número: 205050745, de la Maestría de Derecho Penal, de la Universidad Internacional de las Américas (UIA). Es Todo, firmo en Grecia a las 13:00 horas del día 8 del mes de Diciembre de 2020.**



Dirigido a Fiscales, para identificar aportes vivenciales en el abordaje de los delitos informáticos en el marco jurídico costarricense, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente **José Benjamin Hidalgo Durán**, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Lic. Carlos Arias Córdoba. Fiscal de la República.

1. ¿Qué es un ciberdelito o delito informático?

Es aquella acción cometida por una persona con el fin de ocasionar un perjuicio patrimonial antijurídico, un perjuicio a la intimidad y por ende a la moral de una persona y/o además puede tener también fines de alarma social, esto con la utilización de cualquier medio tecnológico, sistema o programa informático incluyendo cualquier red social, donde también entran en juego el ardid o la capacidad que tiene el sujeto activo de engañar a las víctimas para obtener información sensible que le permita acceder a sus fines; el aprovechamiento de puestos de confianza donde al actor se le facilite el acceso a sistemas informáticos financieros o; también se valgan de las habilidades y conocimientos técnicos para acceder a información o a los sistemas informáticos.

Si bien el Código Penal contiene en su sección VIII una serie de tipos penales denominados Delitos informáticos y conexos, de naturaleza fraudulenta, consideramos (opinamos) que algunos delitos contra la intimidad, en la que se utilizan medios tecnológicos, también son delitos informáticos, como por ejemplo el delito de Violación de datos personales.

2. ¿Qué ley regula los delitos informáticos en Costa Rica?

El Código Penal y a nivel convencional, Convenio de Budapest sobre ciberdelincuencia.

3. ¿Quién comete delitos informáticos?

El código dice que 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. La acción típica consiste, con el uso de medios informáticos, procesar información que de alguna forma procure beneficio económico al autor o a un tercero, mediante distracción de fondos, generación de errores contables, maquillaje de informes, etc. Pero también están aquellas acciones en las que el autor suplante una identidad, una página Web, o utilice redes sociales para violentar la intimidad de las personas o incluso hasta procurar un contacto sexual con personas menores de edad.

4. ¿Quién es el sujeto pasivo en los delitos informáticos?

Es la persona que cae en el engaño de brindar datos personales, a quienes se les ve violentado el acceso a sus datos financieros informáticos o a quienes se le violente el derecho a su intimidad, siendo que el autor acceda a sus cuentas de correo electrónico y hasta redes sociales.

5. Según su experiencia. ¿Cuáles son los delitos informáticos más frecuentes que cometen los delincuentes?

Fraudulentos, por lo general la estafa informática. En el Circuito Judicial de Pérez Zeledón es frecuente los delitos donde el delincuente confecciona una página de Facebook donde se hace pasar como prestamista de dinero, se publicita en diferentes grupos, accede a datos personales de sus víctimas, y ya sea que accede a sus datos para ingresar a las cuentas bancarias en línea o engaña a las personas para que le depositen sumas de dinero por los servicios que hace creer que brinda en redes sociales. En materia sexual, es muy frecuente el delito de seducción o encuentros con menores por medios electrónicos.

6. ¿Es difícil identificar a los sujetos activos de delitos informáticos?

Sí, porque por ejemplo en las defraudaciones, cuando los montos de dinero se desvían hacía una cuenta bancaria determinada, no se puede atribuir la responsabilidad penal al dueño de la cuenta bancaria, es decir, no se puede probar que el dueño de la cuenta fue quien realizó el fraude; además, muchas veces estos delincuentes actúan bajo un seudónimo y la única forma de poder saber más o menos donde se originó la acción, es mediante la dirección IP, pero son aspectos técnicos que muchas veces pueden ser evadidos por los delincuentes.

7. ¿Cuál es el mayor problema a la hora de enfrentar un proceso Judicial por delitos informáticos?

Muchas veces se tienen que solicitar los levantamientos de secretos bancarios ante el juez penal, encontrar y decomisar los equipos de cómputo, posteriormente se debe señalar fecha y hora para hacer apertura esa evidencia y que el equipo especial del OIJ, realice las pericias necesarias para vincular a los imputados en el delito. Todo esto lleva mucho tiempo y requiere del análisis de muchos indicios.

8. Según su experiencia, en caso de existir problemas. ¿Cuáles son los principales impedimentos u obstáculos para poder procesar penalmente a los delincuentes informáticos?

Principalmente identificar a los delincuentes, cuando se da un fraude por haber ingresado al sistema informático bancario de una persona, no se puede determinar con certeza qué persona lo hizo, a partir de ahí la investigación se vuelve muy compleja.

9. ¿Considera usted que las universidades deberían incluir la materia de delitos informáticos?

Sí, en términos generales deberían de dar una inducción sobre las nuevas modalidades de esta delincuencia, la cual cambia día con día.

10. Con respecto al tema de los ciberdelitos y el procedimiento penal en Costa Rica. ¿Qué recomendaciones consideraría para mejorarlo

Dentro del Ministerio Público y el Organismo de Investigación Judicial, existe en San José, Unidades especializadas que tramitan este tipo de delitos, supongo que reciben constante capacitación al respecto, pero a nivel de Judicatura y de los Circuitos Judiciales de otras zonas, no existe esta especialización. Además, a nivel universitario o por medio del Colegio de Abogados, se debería incentivar la elaboración de cursos de actualización jurídica sobre estos temas.

11. ¿Según su conocimiento los problemas de seguridad han hecho cambiar en la población la forma en que se utiliza el internet?

No, mi opinión es que la población sigue siendo ingenua ante este tipo de delincuencia. Aquí juegan varios elementos: la capacidad de engañar del delincuente, su habilidad en manejar los sistemas informáticos, el valerse de tener una posición en una institución, la debilidad en la seguridad de los sistemas bancarios y la vulnerabilidad de la víctima.

A lo último nos referimos que muchas veces las víctimas son personas con problemas financieros que necesitan una solución urgente e inmediata y al ser contactados por este tipo de delincuente, su condición de necesidad no les permite determinar muchas veces en el error al que les inducen.

Consentimiento informado. Lic. Carlos Arias Córdoba. Fiscal de la República.

CONSENTIMIENTO INFORMADO

Yo Carlos Arias Córdoba, con cédula de identidad número: 1-1218-0859, autorizó que se ponga mi nombre, que se grave mi voz, para efectos de la investigación, la cual es: LA ESPECIFICIDAD DE CONOCIMIENTOS EN LOS DELITOS INFORMÁTICOS, del estudiante: JOSE BENJAMIN HIDALGO DURAN, cedula de identidad número: 205050745, de la Maestría de Derecho Penal, de la Universidad Internacional de las Américas (UIA). Es Todo, firmo en San José a las 10:00 horas del día 07 del mes de enero de 2021.

Carlos Arias Córdoba

FIRMA Digital.

Dirigido a Fiscales, para identificar aportes vivenciales en el abordaje de los delitos informáticos en el marco jurídico costarricense, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente **José Benjamin Hidalgo Durán**, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista Lic. Ovidio González Cruz. Fiscal de la República.

1) ¿Qué es un ciberdelito o delito informático?

-Ciberdelito o delito informático, es aquella acción ilícita que se comete a través de un dispositivo electrónico, llámese una computadora, un teléfono celular, un ordenador, en ese sentido la mayoría de países no han establecido un concepto generalizado para toda la región pero por lo menos a nivel de conceptos ese es el que se maneja una acción ilícita la cual se comete por medio de un ordenador o dispositivo electrónico como te indique anteriormente pero esa el base utilizar esa herramienta un dispositivo electrónico.

2) ¿Cuál es el perfil de quien comete delitos informáticos?

-Vieras que en principio obviamente tiene que tener un concepto básico, saber utilizar un ordenador, más, sin embargo, los tipos de delitos van en escala ya que hay personas que cometen delitos por ejemplo aquí en Costa Rica que es el más conocido por medio de ingeniería social, que se hacen pasar por personeros del Banco Nacional, del Banco de Costa Rica, de Hacienda y pues sacan información a las personas.

-No existe un perfil o una determinada persona, porque se cometen delitos de delitos, incluso llámese la violación de datos personales o la creación de un perfil donde suplantas la identidad de otra persona, en donde no se adquiere gran conocimiento nada más tomas mis datos yo tomo los tuyos y creo un perfil y de ahí empiezo a estafar, pero por lo menos si hay tendencias en el sentido que hay personas que entre más conocimiento es más grande la estafa, pero por lo

menos la persona que comete un delito debe tener al menos un conocimiento básico en redes y utilización de un ordenador.

3) Según su experiencia ¿cuáles son los delitos informáticos más frecuentes que se cometen?

-Aquí en Costa Rica el delito más común estadísticamente es el delito de estafa informática, ese el delito es el que se comete más a nivel país, vieras que en ese sentido de acuerdo a todas las investigaciones que se han realizado a veces es muy difícil determinar quién es el frentiador, quien es el que realizó la llamada, el que hizo toda la ingeniería social, lo que si se llega a determinar son los cuenta destinos, donde va ese dinero depositado, en ese sentido pues ya existe el año pasado creo que hubieron dos o tres condenas a personas que prestaron su cuenta para realizar este tipo de estafa, pero el delito más común por lo menos aquí en Costa Rica y se ha visto en otros países ***es la estafa informática.***

4) ¿Es difícil identificar al actor propiamente de esos delitos informáticos?

-Vieras que igualmente es un poco difícil pero no del todo, porque aquí igualmente se ha logrado identificar por medio de… Es que los proveedores de servicio actualmente o esas personas que actualmente usan un tipo de herramienta, a veces logran disfrazar los números de IP, porque obviamente sabemos que con un numero de IP si sabemos que en el caso de una persona que está realizando una estafa informática con un número de IPE estático, de esos que te da Kolbi y Telecable, entonces a veces es fácil porque son personas que tienen poco conocimiento entonces puedes llegar a determinar el número de IP, existen también personas que ya tienen mucho conocimiento que lo que hacen es que solicitan servicios a un proveedor de los Estados Unidos, entonces van en cadena, de los Estados Unidos te manda China, de China te manda Rusia, entonces ahí vas como escondiendo ese número de IP y al final tal vez se logra determinar que el número

de IP se encuentra en los Estados Unidos, pero a veces esas personas logran disfrazar o encriptar esa información y es un poco difícil ya son personas que tienen amplio conocimiento en este delito del ciber crimen, más sin embargo aquí en Costa Rica si se ha logrado identificar que esas personas que tienen poco conocimiento, apenas están empezando o no tienen ese cuidado y se han logrado identificar por el número de IP, también cuando utilizas teléfonos celulares para cometer estafas, si es un poco más difícil, porque ahí utilizas un numero de IP dinámico, en donde cada vez que te conectes a internet ese proveedor de servicio te va a dar un numero de IP diferente, entonces te conectas en este momento en internet te da un numero de IP si te desconectas y te volvés a conectar entre diez o quince minutos te vuelve a dar otro número de IP, entonces para ellos es más difícil porque no llevan una bitácora en donde digan mira este número de IP se le dio a Ovidio a tal hora, entonces es un poco más difícil por esa IP cambiante, pero en cuanto los IP fijos que se utiliza normalmente en las casa de habitación si se ha logrado determinar a las personas, porque ya atreves de solicitar información te dan información valiosa como cuál fue el aparato electrónico, de que marca, pero ***si se ha logrado determinar aquí en Costa Rica quien es la persona que realiza esa estafa***, por lo menos el frentiador verdad.

5) ¿Cuál es el mayor problema judicialmente a la hora de afrontar un proceso judicial por este tipo de delitos?

-En cuanto el delito informático es por la evidencia, que hay que recolectar evidencia digital y en ese sentido como no es un delito común, normalmente en la delincuencia común ya sabes que hay que hacer o por lo menos ya viene establecido en la norma procesal cuales son los pasos o las pruebas que ocupas para demostrar, ese tipo de delito, en cambio en cuanto a ciber crimen vieras que es una evidencia que a veces es muy difícil conseguir en el sentido que hay personas que nada más utilizaron un dispositivo electrónico para cometer esa estafa y lo

desecharon, entonces el problema más que todo es por la recolección porque como todo es por medio digital seria primeramente descubrir ese número de IP, después un posible allanamiento y también a nivel de Ministerio Publico también ha sido un problema porque a veces nosotros como Ministerio Publico, el Ministerio ha estado realizando mucha capacitación para los fiscales, pero lo que pasa es que en un tiempo pues no se estaba capacitando la Judicatura, entonces en ese momento nada hacías con tener todo ese amplio conocimiento como fiscal, si al final las solicitudes tenía que hacérselas a la autoridad jurisdiccional y ellos tal vez no tenían ese conocimiento, entonces ellos decían como voy a otorgar una solicitud de allanamiento si procesalmente no tenemos nada, si es legal o no es legal, en la actualidad ese chip ha venido cambiando, entonces ahora va paralelamente se dan las capacitaciones, Ministerio Publico y Judicatura entonces ellos ya van obteniendo conocimiento en el tema y se les hace más fácil realizar ese tipo de diligencia ordenarla porque también para ellos habían una duda como de que puedo ordenar o que no puedo ordenar, porque digamos a nivel procesal del cibercrimen a veces hay que interpretar la norma ampliamente, pero como son delitos totalmente nuevos el problema es entonces a la recolección de la evidencia digital que es una información que fácilmente una persona puede hacer la estafa y borrar toda la información y la otra es el conocimiento que no tenía o no estaba teniendo en algunos momentos la Judicatura tal vez a veces nos rechazaban las solicitudes al no tener conocimiento, nos rechazaban las solicitudes de allanamientos, intervenciones, aperturas o extracción de esa información, entonces por ahí había un problema que ya se ha sido solucionando poco a poco.

6) El hecho de que los tipos penales no estén concentrados ¿no crea algún problema?

-De hecho, porque obviamente tenemos varios articulados en el código penal pero a criterio de nosotros tiene que haber una ley específica donde se regule de forma específica ese tipo de delitos, que exista un cuerpo normativo que se encargue únicamente de eso porque digamos

hay varias figuras que ahorita no se han contemplado como los accesos ilícitos porque si existe un primer tema de todos los daños informáticos, el sabotaje informático, posteriormente tenemos otro tema de la violación de datos personales, de la captación, y la suplantación y todo pero si como tal hay acciones ilícitas que no están contempladas como los accesos ilícitos que no se encuentra estipulado en el código penal, para mi si tiene que haber un cuerpo normativo que se refiera de forma amplia a ese tipo de delitos y no tenerlo repartidos en el Código Penal por títulos que no están juntos, a criterio de esta representación ***si es necesario que exista un cuerpo normativo que regule esa materia***.

7) ¿La terminología del tipo penal, crea algún problema en los operadores de justicia según su experiencia?

-Si claro, porque como te lo indique anteriormente, cuando nosotros empezamos a hacer solicitudes de allanamiento, entonces nosotros le decíamos a la autoridad jurisdiccional vea es que nosotros identificamos a esta persona por medio del IP, que es un IP que el solicito los servicios en tal telefonía o en tal operadora de servicios y por ahí fue que se identificó, entonces digamos ellos decían ¿Qué es un numero de IP? Entonces es dinámico o es estático, para mucha gente calzaba un tipo de información porque la terminología es amplia, normalmente cada vez aparecen más virus, que es en sí entonces esa terminología que es amplia y es cambiante día a día, pues obviamente para las personas que no están actualizadas causan un tipo de información porque las personas dicen bueno esta persona está utilizando un proxy pudo ocultarlo, entonces toda esa terminología para le gente causa algún tipo de confusión, en el sentido de que si no sabes que es ese tipo de terminología te va a costar desinformación porque en realidad te van a hacer una solicitud donde tal vez el fiscal va a utilizar términos que tal vez el juez penal no conoce, en ese sentido lo que hacíamos nosotros era hacer la solicitud y previo a que se resolviera íbamos con el

investigador, íbamos con la gente de la sección de ciber crimen y nos sentábamos y le explicábamos de que se trataba, como se identificó la persona, pues si obviamente la **terminología causo y causa gran confusión para los operadores del derecho**.

8) ¿Deberían las Universidades preparar a los estudiantes de derecho en esta materia de delitos informáticos?

-Sí, para mi vea Licenciado, ya tiene que ser una materia en específico que incluyan las universidades incluso tanto en las universidades como en la unidad de capacitación cuando se prepara a los fiscales, ya el año pasado la unidad de capacitación ya incluyo una partecita para explicarle a los fiscales que es ciber crimen, pero también a nivel de universidad ya para mi tiene que ser una materia casi que exigida en el sentido de que ahorita en la actualidad, en la delincuencia por decirlo en lenguaje popular es el boom, entonces ya los operadores de derecho tienen que venir con algún tipo de conocimiento aunque sea básico en que consiste el asunto del ciber crimen, es algo que ya para mi es esencial que lo den las universidades y que obviamente a la hora de que si vas a hacer parte de la defensa publica, de la judicatura o del Ministerio Publico, también en esa capacitación que te van a dar tienen que incluida este tipo de materia.

9) Con respecto a los ciber delitos y delitos informáticos ¿qué recomendaciones daría para mejorarlo?

- Bueno, normalmente a veces el Ministerio Publico o dependiendo el departamento donde este yo siento que este primero tenemos que leer, que informarnos, que preguntar, no es en todas las fiscalías donde se tramita este delito de forma adecuada, ***para mi hay que leer, informarse, consultar*** en jurisprudencia es poco lo que hay, porque normalmente uno dice bueno mira tengo este delito de administración fraudulenta entonces si no comprendes un poco te metes y vas a encontrar un montón de ese tipo de delitos, pero ya en ciber crimen es poca la jurisprudencia que

hay, ya en ese sentido yo lo que le dije a la gente es que se informen nosotros en la actualidad en la unidad de capacitación se está realizando un proyecto para realizar un protocolo para abordar esta materia de forma general en todas las fiscalías del país, entonces nos hemos dado la tarea de revisar derecho comparado tanto de la norma como de las buenas prácticas entonces también si las personas tienen amistades o conocidos en otros países entonces por lo menos que consulten ante las buenas prácticas, mira que realizan con este tipo de delito ustedes que hacen, entonces en ese sentido para mí, licenciado, tenemos que informarnos, tenemos que leer, tenemos que preguntar, en el caso de nosotros tenemos una sección de ciber crimen, hacer las consultas, ver qué tipo de herramientas tienen, que se ocupa, para mi digamos si tenemos para un mejor abordaje tener eso en cuenta porque si el Ministerio Publico no te ha capacitado tienes que ver la forma de capacitarte vos mismo preguntando a nivel nacional a través de la fiscalía, a los dos compañeros que han tramitado este tipo de delito para un mejor abordaje y si tienes la oportunidad y tienes amigos en otros países pues igualmente hacerles la consulta y esas buenas prácticas ponerlas a trabajar aquí en el país.

10) Respecto a la tipicidad del tipo penal de la estafa que generalmente se utiliza el 216 bis o el 217 bis ¿Existe algún problema en la tipicidad?

-No, en cuanto la tipicidad porque el 217 bis lo que te dice es que ya utilizando… e la estafa del 216 es la pura y simple digamos la que no utilizas ningún tipo de herramienta tecnológica nada más una simple llamada, la llamada no influyo como toda esta plataforma que existe en el marketing como OLX o eso que nada más te pusiste de acuerdo con una persona que le ibas a vender un artículo y al final le dijiste a esa persona que te depositara y al final no enviaste el artículo, entonces obviamente es una estafa pura y simple, utilizaste un medio tecnológico únicamente para hacer la llamada ya la persona fue voluntariamente a hacer el depósito.

-En cuanto al 217 bis que es el que antes se llamaba fraude informático y ahora se llama estafa informática en ese sentido si ya tienes que utilizar un medio tecnológico, como te indique anteriormente que es cuando las personas se hacen pasar por personal del Banco y ya ahí si ocupan la clave dinámica, el token, ocupan toda esa información para ya ingresar a tu cuenta y de ahí pasar dinero a otras cuentas, entonces el 217 bis es como ya la estafa informática en su máximo esplendor en donde si utilizas una herramienta tecnológica para acceder a las cuentas de esa persona o para acceder a la información de esa persona.

-Pero no en cuento a la diferencia, de esos dos tipos penales no tenemos ningún problema.

Consentimiento informado. Lic. Ovidio González Cruz. Fiscal de la República.

CONSENTIMIENTO INFORMADO

Yo OVIDIO GONZALEZ CRUZ, con cédula de identidad número: 205010040, autorizó que se ponga mi nombre, que se grave mi voz, para efectos de la investigación, la cual es: LA ESPECIFICIDAD DE CONOCIMIENTOS EN LOS DELITOS INFORMÁTICOS, del estudiante: JOSE BENJAMIN HIDALGO DURAN, cedula de identidad número: 205050745, de la Maestria de Derecho Penal, de la Universidad Internacional de las Américas (UIA). Es Todo, firmo en San José a las 7:00 horas del dia 10 del mes de Diciembre de 2020.

FIRMA.

Dirigido a profesional en informática y derecho, para identificar aportes vivenciales en el abordaje de los delitos informáticos desde el punto de vista de un especialista en informática y derecho, para la realización de la **tesis para optar por el Grado de Maestría en Derecho con énfasis en Derecho Penal,** del Proponente **José Benjamin Hidalgo Durán**, en la Universidad de las Américas, año 2020-2021. Los datos recopilados se utilizarán únicamente para el fin establecido.

Entrevista al Master Roberto Lemaître Picado.

1) ¿Qué es un ciberdelito o delito informático?

- Un delito es algo típico, antijurídico, culpable, que le estamos agregando elementos del área tecnológica, en mi libro pongo una definición, ya que hay varias definiciones, hasta el momento no hay una definición estándar, pero yo lo defino como: ***"aquella acción típica antijurídica culpable realizada por medios informáticos para eliminar los datos de un dispositivo informático, tanto en el ámbito jurídico como en lo tecnológico".***

2) ¿Qué ley regula los delitos informáticos en Costa Rica?

- Principalmente las vamos a encontrar en el código penal, no tenemos una ley especializada ni un código especializado, sino que son reformas que se han hecho a nuestro código penal, se han integrado dentro del marco penal.

3) ¿Debería de haber una ley específica para los delitos informáticos?

-Como te digo está integrado dentro del código penal, ya tenemos marcos legales avanzados en materia de delitos informáticos, del que mejor salimos beneficiados a nivel internacional es el "***Marco jurídico en materia de tecnologías y delitos informáticos."***

4) Considera usted que está bien ordenado el articulado del código penal o debería de estar más concentrado.

-Eso es una praxis, en los que los países deciden como tenerlo, hay países que deciden tener una norma aparte especializada, otros una norma integrada, "***lo importante es que estén contemplados"*** porque dentro de nuestro contexto de ciber sociedad y cualquier país se encuentran

situaciones que afectan a los ciudadanos, entonces si considero importante es que se requiere estar actualizados con las situaciones actuales, ya que los avances tecnológicos van muy rápido, entonces estar revisando y actualizando la normativa desde un punto de vista equilibrado ***tanto en lo jurídico como en lo tecnológico***, ya que si no comprendes el mundo técnico, es muy lógico desde el punto de vista jurídico pero no sirve para nada en el punto de vista técnico, no tiene sentido, por ende no se va a poder realizar, entonces si no entiendes como ocurre, no entiendes el ambiente de internet si no entiendes como ocurre un ciber delito, desarrollas tipos penales que desde el punto de vista jurídico decís está perfecto tiene los verbos, tiene la acción, tiene la pena pero si lo ves desde los ojos técnicos decís si pero esto no va a poder funcionar, este delito no se va a poder perseguir, este delito no cumple ciertos aspectos técnicos y eso lo hemos visto con las figuras jurídicas que se crearon en el 2001 con las normativas de delitos informáticos que tuvo el país, ya que según la estadística llegaban 100 a juicio y se condenaban a 8, ya que tenía muchos vacíos dentro de la figura.

-Hay un tema de trabajo interdisciplinario que los abogados somos muy quitados a ese tema porque creemos que esto es solo con ojos jurídicos, cuando indiscutiblemente no lo es, necesitamos verlo en las dos áreas.

5) Generalmente ¿Quién es el que comete el delito informático o cuál es el perfil?

-Hay muchos perfiles, puede ser gente con un alto grado de conocimiento en estas acciones, gente por diversión, pero realmente el ciber crimen ahora está mezclado con personas muy técnicas o personas nada técnicas que contratan servicios de ciber crimen ya que ahora se ofrece como un servicio, te ofrecen herramientas para realizar ataques, robar credenciales etc.… personas que por el puesto que ocupan aprovechan para robar información, no podemos hacer un perfil exacto,

porque ahora con la tecnología las acciones delictuales tecnológicas es muy posible que las haga cualquier perfil de persona.

-Por ejemplo, si a vos te llega una información por *WhatsApp* que solo era para vos y la compartiste a alguien sin autorización ya comiste violación de comunicaciones y no ocupaste ser un genio de la informática para ser eso, si tenemos situaciones más avanzadas que si implican un nivel técnico mucho mayor, los temas de estafa, suplantación de identidad.

"La capacidad de cometer estos delitos puede realizarla cualquier persona que quiera hacer una acción para afectar a alguien".

6) El sujeto pasivo generalmente ¿quién es o cómo se puede definir?

"El sujeto pasivo es la persona que sufre la afectación".

- Entre los grupos más vulnerables contaríamos en Costa Rica por ejemplo hemos visto las últimas semanas y a nivel mundial por violación del uso imagen, de imágenes íntimas de mujeres, pornografía con menores, adultos mayores ya que están más expuestos a situaciones que aprovechen ese desconocimiento y que los pueden engañar más fácilmente con llamadas, con mensajes etc.…

7) ¿Según su experiencia cuáles son los delitos informáticos que se cometen más frecuentemente en el periodo 2019-2020?

-Hay varios temas interesantes, las estadísticas dicen que la estafa informática y suplantación de identidad son los delitos más denunciados en el 2019 y 2020.

-Aprovechando la situación de pandemia las estafas informáticas han sido uno de los temas que más han crecido tanto que las estadísticas a nivel mundial dicen que esto ha aumentado un 400% a nivel mundial.

-En Costa Rica hace poco el poder judicial daba unas estadísticas de aumentos considerables, pero si la estafa informática sigue siendo el pilar este año.

-Aparte por el tema de teletrabajo la gente desde sus casas con medios digitales donde se aprovechan de esta información para buscar engañarlos.

8) ¿Es difícil identificar a los sujetos activos de los delitos informáticos?

-Sí, es complejo, aunque no imposible, es más complejo porque los medios digitales hacen que sea más difícil, se ocupa pedir mucha más colaboración de intermediarios por decirlo así ya que la información de diferentes pruebas puede estar tanto en equipos o servidores que estén aquí o que estén fuera del país por eso la relación internacional se vuelve tan importante como lo es la Convención de ciber delincuencia ***"Budapest".***

-Las autoridades judiciales deben de contar con una red de colaboración 24/7 porque no solo es la investigación sino la posibilidad de perder pruebas digitales es mucho más fácil en estos medios que se borren, que se desaparezcan etc.…

-Pedir la colaboración del país firmante de la convección Budapest facilita la ayuda para que se guarden las pruebas referentes al caso en un corto plazo mientras se hacen todos los procedimientos, entonces la colaboración internacional se vuelve fundamental, jurídicos agiles se vuelven fundamentales, no los tradicionales, los agiles ya que se ocupa mucha colaboración para hacer esa persecución.

9) Según su experiencia en caso de existir problemas ¿cuáles son principales impedimentos u obstáculos?

-Creo que los retos que se presentan son a la hora de tener las pruebas.

-Obstáculos de entendimiento de este tipo de delitos por parte de jueces, fiscales y abogados en general.

-Más complejo es entender cuál figura aplica, cómo aplica y porqué, para poder procesar mejor este tipo de casos.

-También hay un reto de que la gente conozca estos delitos para que denuncien ya que tal vez no saben que puede procesarse todo lo que pudiera hacerse.

-La sección de delitos informáticos ocupa más gente y más recursos para ser mucho más efectiva ya que hay una saturación gigantesca.

10) ¿Deberían las universidades en general tener al menos una materia sobre delitos informáticos?

-Efectivamente, las universidades deberían incluir algún tipo de estos cursos, muy pocas lo incluyen, de las pocas que he visto la ***Libre de Derecho*** sé que lo incluye, yo soy docente en la ***Universidad De Costa Rica*** y veo una incorporación interesante han incluido cursos de informática social, los temas de delitos informáticos pero no hay curso directo de estos temas, para tecnólogos, han facultado cursos para abogados que se llaman digital y tecnologías emergentes, también temas de ciber seguridad donde se mezclan las dos áreas tanto la de abogados como la de informáticos.

-Entonces sí, indiscutiblemente es fundamental que den estos cursos en las Universidades porque se tiene que lograr entender el tipo de delito y el medio digital en cualquier materia que podrías verlo y en algún momento esperaría la maestría en delitos informáticos en el país.

11) Con respecto al tema de ciber delito y al procesamiento penal en Costa Rica ¿qué recomendaciones daría para mejorarlo?

- Yo creo que algunas ya las hemos dicho, pero principalmente, el tema de actualizar nuestro marco normativo, estarlo revisando como digo hemos salido muy bien en calificaciones, te recomiendo ver el reciente informe para el estado de ciber seguridad de toda la región incluido

Costa Rica donde hemos mejorado bastante y de los temas que se han mejorado muchísimo están los marcos legales.

-Es necesario estar haciendo revisiones para estar actualizando el marco y que responda a las situaciones más recientes o a las situaciones de avances tecnológicos.

-Procesalmente en Costa Rica se debe empezar haciendo procedimientos para un mejor entendimiento, procesos que incluyan tecnología, es importante revisar también si los procedimientos están adaptados y pensados para al mundo digital.

-Y el tema fundamental es que jueces, fiscales y abogados en general estén especializados como delitos informáticos que se dediquen solo a eso por la especialidad que se genera ahí.

12) ¿El hecho del conocimiento de problemas de seguridad ha hecho cambiar a la población en la forma que utiliza el internet?

- Yo pienso que la gente ahora está un poco más consiente y eso lo refleja el estudio de la OEA, pero aún falta mucho… ser más consiente de los riesgos, hacer más cultura digital para que la gente tome mayores precauciones digitales que los pueden afectar, esto incluye dos áreas no solo saber el riesgo sino saber utilizar la tecnología, creo que este ha sido un año que la gente ha tomado conciencia, que se han cuidado de estafas de llamadas.

Anexo N° 2. Jurisprudencia.

Resolución n°00494 – 2020. II Circuito Judicial San José.

Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José

Resolución Nª 00494 - 2020

Fecha de la Resolución: 26 de marzo del 2020
Expediente: 16-003520-0059-PE
Redactado por: Gustavo Adolfo Rojas Gutiérrez
Clase de Asunto: Recurso de apelación penal
Analizado por: CENTRO DE INFORMACIÓN JURISPRUDENCIAL
Normativa Internacional: Convención americana sobre derechos humanos, Pacto de San José

Normativa internacional

Sentencia con datos protegidos, de conformidad con la normativa vigente

Contenido de Interés:
Temas (descriptores): Estafa informática
Subtemas (restrictores): Confirmación de absolutoria en caso de imputados acusados de prestar sus cuentas bancarias para recibir dineros de forma ilícita
Tipo de contenido: Voto de mayoría
Rama del derecho: Derecho Penal

"III.-1) Voto del juez Rojas Gutiérrez. [...] Como desprende los hechos, la conducta que se le atribuyó a los encartados, fue la de prestar sus cuentas bancarias y recibir los dineros que se transfirieron en forma ilícita por una tercera persona no identificada, que engañó a la ofendida y se apropió de sus claves electrónicas y realizó los distintos depósitos descritos. Se observa a folio 341 a 342 de la sentencia, los hechos se tuvieron prácticamente por probados, salvo por un aspecto fundamental, el elemento subjetivo doloso (conocimiento y voluntad) de los acusados para la comisión del tipo penal de la estafa informática. [...] No existió un error en cuanto al hecho descrito en el punto cuarto de la acusación, debido a que, como se fundamentó, no fue posible determinar el dolo del imputado [Nombre 011] al presentarse a la sucursal del Banco Nacional de Costa Rica, en San Francisco de Dos Ríos. Si bien resultó llamativo el indicio de que el sindicado se presentara en un plazo muy breve en relación con el depósito que se le realizó, y ello, sirvió para alertar a la funcionaria bancaria, ese elemento no es suficiente para poder acreditar el conocimiento por parte del acusado de la estafa informática que se le realizó a la víctima, por lo que la aplicación del principio universal de la duda razonable fue correcta. Misma situación acontece, con el argumento de que el tribunal no adecuó correctamente la participación de los implicados al delito imputado, por la existencia de una coautoría en aplicación de la teoría funcional del hecho. De conformidad con el artículo 45 del Código Penal, son coautores quienes realicen el hecho punible tipificado conjuntamente con el autor. Ello implica conforme a la teoría del dominio funcional del hecho, expuesta por el recurrente, que se cumplan con tres requisitos, según el profesor Roxin: i.- El requisito objetivo, que es la distribución de funciones, donde el aporte debe ser tan importante, de forma que, al hacer una supresión hipotética, el hecho no se hubiera podido cometer sin él. ii. El requisito subjetivo, que es el plan previo. iii. El requisito negativo, que no sea un delito especial propio, culposo, de omisión o de propia mano. Expuesto lo anterior, la tesis fiscal no puede aceptarse, en primer lugar, porque la acusación no describe la coautoría, ni sus elementos, y como segunda limitación, como se expuso en la sentencia, no existen pruebas ni indiciarias o directas, de la existencia de un plan o acuerdo previo, entre los participantes. Por lo que el indicio de una posible distribución de funciones, donde los encartados prestaron sus cuentas para la comisión del delito de estafa informática es insuficiente, en el caso no fue posible siquiera ligar a los acusados (frenteadores) entre sí, y mucho menos, se ofreció prueba sobre la persona que realizó los actos de engaño y apropiación de las claves

y realizó las transferencias y su relación con ellos. Esa ausencia de material probatorio idóneo, es la que genera la duda razonable, que fue aplicada al caso en concreto. Sobre las condiciones del acusado [Nombre 011], en el sentido que la cuenta fue de reciente apertura en la relación con los hechos delictivos, que recibió dinero de una persona a quien no conocía ni tenía derecho a recibirlo y su puntualidad de presentación a la entidad financiera, si bien son indicios, no son unívocos, y los mismos son insuficientes, por más referencia que se haga a los informes policiales, o la funcionaria del banco que lo atendió, lo cierto es que no es posible acreditar más allá de toda duda razonable, con la certeza positiva requerida, que el encartado tenía conocimiento del delito que se estaba cometiendo y que formaba parte de un plan de autor. Tampoco es cierto que la prueba bancaria se valoró en forma incorrecta. Como se informa en el fallo, esos elementos sugieren la participación de los acusados en los hechos, pero hasta ahí, en el caso concreto, para poder determinar su responsabilidad penal, era necesario otros indicios o pruebas directas, para considerarlos coautores. La fiscalía pretende que, por la circunstancia de que a los implicados se les depositó el dinero en sus cuentas, y ellos en forma independiente, realizaron pagos, retiros, o se presentaron al banco, sea suficiente para estimar el conocimiento y voluntad en el delito de estafa informática, pero, como se dijo, eso un indicio único. Por ello la afirmación del a quo de la necesidad de contar, con antecedentes policiales o algún otro insumo, como el perfil de vida de los endilgados, para poder concluir la existencia del dolo requerido para la comisión del ilícito, no es errónea. En virtud de lo anterior, la resolución cumple con los requisitos de argumentación de conformidad con el numeral 142 del Código Procesal Penal y respeta las reglas de la sana crítica racional. En consecuencia, los alegatos se deben rechazar. 2) Voto de la jueza Vargas González. Estimo que la impugnación debe ser

declarada sin lugar, no por ausencia de indicios para demostrar el dolo de los imputados, sino porque la acusación formulada por el órgano requirente no contiene los elementos necesarios para atribuir a estos una coautoría en el delito de estafa informática. [...] Conviene hacer notar que, solo añadiendo aspectos que la requisitoria no contiene, se podría concluir que existió un plan común, donde quienes prestaban sus cuentas y retiraban los dineros sabían que otro u otros sujetos procedían al despojo del dinero en los términos que apuntan los hechos 2.-, 3.- y 4.- de la acusación (que no son, sino, los del tipo penal de la estafa informática). En este contexto, donde la imputación no contiene la información necesaria para establecer una coautoría, estimo que los reclamos que formula el recurrente deben declararse sin lugar, ya que incluso admitiendo hipotéticamente que hay indicios para establecer que los endilgados actuaron dolosamente, y que no fue por azar o casualidad que recibieron y retiraron el dinero transferido desde la cuenta de la víctima, era inviable el dictado de una condena. Por lo dicho, los alegatos deben rechazarse.

... Ver menos

Texto de la Resolución

Resolución: 20 20-0494
Expediente: 16-003520-0059-PE (14)

TRIBUNAL DE APELACIÓN DE SENTENCIA PENAL. Segundo Circuito Judicial de San José. Goicoechea, al ser las ocho horas cinco minutos, del veintiséis de marzo de dos mil veinte. -

RECURSO DE APELACIÓN interpuesto en la presente causa seguida contra [Nombre 007], [...]; [Nombre 009], [...]; [Nombre 011], [...] y [Nombre 012], [...], por el delito de ESTAFA INFORMÁTICA, en perjuicio de [Nombre 001]. Intervienen en la decisión del recurso, el juez Gustavo Adolfo Rojas Gutiérrez y las juezas Patricia Vargas González, Elizabeth Montero Mena. Se apersonaron en esta sede el licenciado Carlos Castro Sojo, en representación del Ministerio Público; la licenciada Ana Carolina Campos Camacho, en su condición de fiscal de la Unidad de Impugnaciones del Primer Circuito Judicial de San José y la licenciada Vanessa Cascante Alfaro, en su condición de defensora pública del justiciable.

RESULTANDO:

I.- Que mediante sentencia número 1130 -2019, de las quince horas cuarenta minutos del primero de octubre de dos mil diecinueve, el Tribunal Penal del Primer Circuito Judicial de San José, resolvió: " POR TANTO: De conformidad con lo dispuesto en el numerales 39 y 41 de la Constitución Política, 8.2 de la Convención Americana de Derechos Humanas,1, 30, 45, 217 bis del Código Penal , 1, 6, 7, 9, 142, 265, 360, 361, 364, 365 y 366 del Código Procesal Penal se ABSUELVE de toda pena y responsabilidad a [Nombre 011], [Nombre 009], [Nombre 007] Y [Nombre 012] por el delito de ESTAFA INFORMATICA que se le ha venido atribuyendo en perjuicio de [Nombre 024]. Se ordena el cese de cualquier medida cautelar impuesta en contra de los imputados con ocasión a esta causa. Son los gastos del proceso a cargo del Estado. Se ordena agregar al legajo de investigación judicial la evidencia material decomisada. HAGASE SABER MEDIANTE LECTURA " (sic).

II.- Que, contra el anterior pronunciamiento, interpuso recurso de apelación el licenciado Carlos Castro Sojo, en representación de la Fiscalía de Fraudes del Primer Circuito Judicial de San José.

III.- Que verificada la deliberación respectiva de conformidad con lo dispuesto por el artículo 465 del Código Procesal Penal, el Tribunal se planteó las cuestiones formuladas en el recurso de apelación.

IV.- Que en los procedimientos se han observado las prescripciones legales pertinentes. Redacta el juez de Apelación de Sentencia Penal Rojas Gutiérrez; y,

CONSIDERANDO:

I.- El licenciado Carlos Castro Sojo, como representante del Ministerio Público interpuso recurso de apelación en contra de la sentencia N° 1130-2019, dictada por el Tribunal Penal del Primer Circuito Judicial de San José, de las 15:40 horas del 01 de octubre de 2019, en la que se absolvió a los encartados [Nombre 011], [Nombre 012], [Nombre 009] y [Nombre 007], del delito de estafa informática que se le venía atribuyendo. Del estudio del sumario se colige que dicho recurso se presentó en tiempo, conforme al plazo de ley, y de acuerdo con los presupuestos que se requieren para que dicha impugnación posibilite el adecuado y correcto conocimiento de la inconformidad planteada por el gestionante, en orden al examen integral de la sentencia impugnada, tal y como lo establece el artículo 8.2h de la Convención Americana sobre Derechos Humanos, y los artículos 458, 459, 460 y 462 del Código Procesal Penal.

II.- El fiscal Castro Sojo, como primer motivo, reclama una errónea determinación de los hechos probados, específicamente en el punto cuarto, donde el tribunal de mérito tiene como probado que el acusado [Nombre 011] se apersonó a la ventanilla de la agencia del Banco Nacional de Costa Rica, en San Francisco de Dos Ríos, lugar donde fue detenido, omitiendo tener por demostrado que el sindicado se presentó y solicitó el retiro de los fondos que le habían sido transferidos a su cuenta bancaria instantes previos. Agrega que, dentro de la pieza acusatoria, se le imputó a todos los implicados, el facilitar sus cuentas bancarias a sujetos desconocidos, para que las utilizaran como receptoras de los dineros que iba a despojar fraudulentamente a la ofendida [Nombre 001]. Fustiga que, en el caso de [Nombre 011], quedó demostrado con el informe policial 465-IP-SITE-2016 de la Sección de Investigaciones de Turno Extraordinario, que la presencia del encartado en la entidad bancaria fue inmediata en relación con la transferencia, lo que se corroboró con la declaración de la testigo [Nombre 022]. Considera el impugnante, que la prueba evacuada en el contradictorio fue suficiente, para tener por probada la finalidad del acusado [Nombre 011], como parte de sus funciones. De haberse tenido por demostrado correctamente el hecho cuarto del requerimiento fiscal, se hubiese acreditado la participación que fue encomendada al sindicado. Solicita se declare con lugar el reclamo y se anule la sentencia. El fiscal, como segundo motivo,

expone que se dio una inobservancia por parte del a quo, al considerar que lo ocurrido no se adecua al delito de estafa informática previsto y sancionado en el artículo 217 bis del Código Penal. De seguido transcribe extractos de fallo recurrido. De lo expuesto consideró el tribunal de mérito que no se puede atribuir la conducta del tipo penal acusado, solo porque la acción de llamar a la víctima y lograr mediante engaño que la facilitara sus cuentas y claves de acceso y se realizaran las transferencias, la hizo una persona desconocida que se hizo pasar por funcionario bancario. Esa posición, deja de lado la teoría de la "autoría funcional" del profesor Roxin, donde varios sujetos correalizan la ejecución de distintos papeles (funciones), de tal forma que sus aportes al hecho tomados en sí, completan la total realización del tipo. Agrega que, según esta misma teoría de la coautoría, los intervinientes por medio del dominio funcional del hecho, deben compartir la decisión conjunta de realizarlo y cada uno debe aportar una contribución al hecho que, por su importancia, resulte cualificada para el resultado y que vaya más allá de una mera acción preparatoria. Estima el recurrente, que, en este caso en concreto, atendiendo a la "división de papeles" basta entonces que cada coautor aporte una parte necesaria de la ejecución del plan global dentro de una razonable división de trabajo, de ahí que, si quitamos el aporte o participación de los titulares de las cuentas de destino, ese plan global no se va poder realizar. Lo anterior, permite considerar a esas personas coautores del delito de estafa informática, aunque los mismos no hayan realizado las llamadas a las víctimas, ni realizado las transferencias desde la cuenta de la ofendida hacia las suyas. Es claro, que la única forma para que se llevaran a cabo los hechos, es que existiera un acuerdo previo entre la persona que realizó la llamada fraudulenta a la ofendida y las personas que facilitaron sus cuentas para que les transfirieran los dineros. Solicita se anule la sentencia recurrida. Como tercer motivo, se reclama que se dio una errónea valoración de la prueba testimonial de [Nombre 022]. Fustiga que la versión dada fue clara, en el sentido que al observar que el sindicado [Nombre 011], se presentó minutos después de realizado el depósito, le generó sospecha, sumado a que era una persona joven, y que la cuenta de ahorro había sido abierta de manera reciente. Estas circunstancias le hicieron comunicarse con la titular de la cuenta, la señora [Nombre 001], quien negó realizar transacción alguna. En el caso, del imputado [Nombre 011], se dieron indicios para determinar su participación, entre ellos: i.- la reciente apertura de la cuenta bancaria para que le depositaran los dineros de forma fraudulenta; ii- recibir dineros de una persona con la cual no tenía relación alguna, ni derecho a recibirlos; iii- el presentarse a la entidad bancaria a retirar los dineros una vez que tuvo conocimiento que le fueron transferidos. Concluye el recurrente, que, si el tribunal de mérito hubiese valorado el testimonio de Ericka, se hubiese tenido por demostrada la forma de operar de los acusados, el codominio funcional del hecho y el conocimiento de la ilicitud que tenía el encartado [Nombre 011], sobre los dineros que fueron transferidos de forma fraudulenta. Solicita se declare con lugar el motivo. En el cuarto motivo, se expone la inobservancia del deber fundamentación, sobre la valoración de la prueba bancaria. Sostiene que el a quo, para considerar que los acusados eran coautores, estimó que debían tener antecedentes policiales por hechos similares, o bien, para establecer el conocimiento de la ilicitud en la ejecución de los actos que se les imputó. Sumado se estimó sugestiva la información bancaria de las cuentas de los acusados, la que se recopiló mediante el levantamiento del secreto bancario. Esa posición no se comparte, ya que es erróneo exigir antecedentes, lo que no puede ser un requisito para cometer el delito. Por otro lado, no se valoró la información bancaria en forma correcta, en ese sentido, las fechas de apertura, los movimientos bancarios antes, durante y después de las transacciones fraudulentas, las horas de las transferencias versus el momento que se presentaron los endilgados a las entidades bancarias. Esa ponderación de la prueba indiciaria, era necesaria, pero el tribunal de mérito no se esmeró, sino que más bien realizó un análisis superficial y general. Solicita se declare la nulidad de la sentencia, y se ordene juicio de reenvío. Se dio audiencia a las partes del recurso. La licenciada Vanessa Cascante Alfaro en su condición de defensora pública, manifestó: sobre el primero motivo, este razonamiento no es correcto, si se analiza la sentencia impugnada se observa que el ente ministerial no lleva razón. El juzgador no compartió el proceder del Ministerio Público en el sentido que esa acción daba cuenta de forma inequívoca que su representado, había participado con conocimiento y voluntad en el delito de estafa, ni que conociera que el dinero procedía de una conducta delictiva. En cuanto al segundo motivo, si se analiza con detenimiento el razonamiento del tribunal sentenciador, el mismo resulta acertado, ya que no se atribuyó a los encartados la comisión de los verbos típicos de la conducta acusada, y si bien, el Ministerio Público hace referencia a la coautoría, lo cierto del caso es que no hay elemento probatorio alguno del que se desprenda el acuerdo previo de voluntades en el plan común. Le resulta extraño que la fiscalía solamente hizo referencia a la coautoría en el recurso de apelación, mientras que en el juicio adujo la existencia de un dolo eventual, argumento erróneo ya que el delito de estafa informática, al igual que el tipo simple, es un tipo penal que solo admite dolo directo. Sobre el tercer motivo, la señora Ericka fue enfática en referir que no sabía quién había realizado la llamada

telefónica a través de la cual se realizó la transferencia ilícita, tampoco pudo dar cuenta de que esa persona tuviera contacto con los imputados, por ello, el juzgador le otorgó el alcance probatorio a la testigo y lo que alega el fiscal es una disconformidad con el acertado proceder del tribunal. Acerca del cuarto motivo, fustiga que el ente fiscal pretenda que el a quo, desprenda determinados aspectos que para él resultaban importantes, pero sin que existan elementos probatorios que los respalden. Es correcto que se expresara por parte del tribunal de mérito, la necesidad de contar con otros elementos, como los antecedentes policiales, o algún otro indicio unívoco, máxime cuando el fiscal, sostiene que los encartados, forman parte de una organización criminal, aspectos que no tuvo respaldo probatorio alguno. Solicita se rechacen los motivos de apelación.III. - Por la conexidad de los motivos, se conocen en forma conjunta. Por mayoría (con el voto salvado de la jueza Montero Mena), se declaran sin lugar los reclamos. Si bien el juez Rojas Gutiérrez y la jueza Vargas González optan por declarar sin lugar la impugnación, al tener razones distintas para arribar a esa conclusión, estas se expondrán por separado. 1) Voto del juez Rojas Gutiérrez. Una vez revisada en forma integral la sentencia impugnada, que se encuentra de folios 384 a 400 del legajo principal, se constata que los yerros, que reclama el fiscal, no acontecieron. Si bien los motivos, se presentan por separado, al dar lectura de los mismos, estos redundan en el mismo aspecto, por ello se abordarán de manera conjunta. Es importante tener claros los hechos acusados: ""“1. Previo a los hechos que se indicarán una persona hasta el momento sin identificar, contactó a los acusados [Nombre 011], [Nombre 009], [Nombre 007] y [Nombre 012], a fin de que le facilitaran el número de su cuenta bancaria, para así utilizar esas cuentas como cuentas receptoras de los dineros que se enviarían haciendo uso abusivo y no autorizado de los datos que ilegítimamente una persona obtendría de la cuenta bancaria del Banco Nacional de la ofendida [Nombre 001]. Los acusados accedieron a la petición de la persona de calidades desconocidas y le facilitaron a este los números de sus cuentas bancarias. 2. El 01 de julio del 2016, a eso de las 10:00 horas aproximadamente, la ofendida [Nombre 001], recibió una llamada de una persona de identidad desconocida, quien indicó estar interesado en comprar varios muebles que la ofendida tenía a la venta en la página OLX. El sujeto le dijo a la ofendida que el pago de los muebles debía realizarse por medio de una transferencia SINPE, que para realizarla debía hacer una teleconferencia con un supuesto funcionario del Banco Nacional de Costa Rica; en ese instante, se introdujo en la llamada un segundo sujeto, quien antecedido de la música publicitaria del Banco Nacional de Costa Rica indicó ser funcionario de dicho Banco y que en ese momento se enlazaba a la conversación telefónica, para realizar la transferencia de dinero para el pago de los muebles, cuestión falsa pues lo que pretendían esos sujetos era obtener los datos que utiliza la ofendida para accesar a su cuenta y realizar transferencias electrónicas. 3. Para darle confianza a la ofendida, el supuesto funcionario del banco le pidió varios datos al sujeto de calidades desconocidas, tales como los datos de sus tarjetas, el PIN, datos que sujeto le proporcionó. Luego el supuesto funcionario del banco le pidió a la ofendida iguales datos, pero como la ofendida no poseía la clave del cajero el sujeto le pidió las claves para accesar sus cuentas por internet, cuestión a la que accedió la ofendida 4. De forma simultánea mientras la ofendida hablaba con los sujetos conforme le proporcionaba el número de identificación así como de la contraseña de acceso a sus cuentas bancarias, el supuesto funcionario del banco, incidió en el procesamiento de datos del sistema informático del banco de Nacional de Costa Rica, ya que utilizando abusivamente los datos de los que se impuso ilícitamente, acceso a la cuenta en dólares [Valor 002] y colones [Valor 003] del Banco Nacional de Costa Rica propiedad de [Nombre 024] cuya autorizada es la ofendida [Nombre 001] y realizó cuatro transferencias electrónicas por internet banking: por la suma de $5.078.49 dólares (equivalente de ¢2.750.000 millones de colones) hacia la cuenta [Valor 001] del Banco Nacional de Costa Rica, cuyo titular es el imputado [Nombre 011], por la suma de $3.693.44 dólares (equivalente de ¢2.000.000 millones de colones) hacia la cuenta [Valor 004] del Banco Nacional de Costa Rica, cuyo titular es la imputada [Nombre 007], por la suma de $4.616.81 dólares, (equivalente de ¢2.500.000 millones de colones) hacia la cuenta [Valor 005] del Banco Nacional de Costa Rica, cuyo titular es el imputado [Nombre 012], a las 11:14 horas aproximadamente, por la suma de ¢950.000 y ¢1.000.000 de colones hacia la cuenta 10000015201000151 del Banco Nacional de Costa Rica, cuyo titular es la imputada [Nombre 009]. 5. Una vez acreditados los fondos en las cuentas de los acusados, ese mismo día, los imputados conociendo el origen ilegítimo de dinero, hicieron el retiro de los dineros transferidos, en el caso de la acusada [Nombre 009], al ser las 11:49 horas aproximadamente, se apersonó a la ventanilla de la Agencia del Banco de Costa Rica, oficina 377, ubicado en San José y retiró la suma de ¢1.500.000 millones de colones, de seguido ese mismo día, al ser las 11:55 horas en el cajero automático del mismo banco, retiró en dos tractos la suma de ¢250.000 y ¢200.000 colones. Asimismo, el acusado [Nombre 011], se apersonó a la ventanilla de la agencia del Banco Nacional de Costa Rica, en San Francisco de dos Ríos gestionó el retiro de los dineros transferidos ilícitamente, sin embargo, el banco detectó de fraude y bloqueó la cuenta del acusado, siendo

detenido en el sitio. Del mismo modo el acusado [Nombre 012], se apersonó a la ventanilla del Banco Nacional de Costa Rica, oficinas Centrales en San José, gestionó el retiro de los dineros transferidos ilícitamente, sin embargo el banco detectó el fraude y bloqueó la cuenta del acusado, siendo detenido en el sitio y la imputada [Nombre 007] se apersonó a la ventanilla del Banco Nacional de Costa Rica, en Heredia, gestionó el retiro de los dineros transferidos ilícitamente, sin embargo el banco detectó el fraude y bloqueó la cuenta de la acusado." (cfr. acusación de folio 170 a 172). Como desprende los hechos, la conducta que se le atribuyó a los encartados, fue la de prestar sus cuentas bancarias y recibir los dineros que se transfirieron en forma ilícita por una tercera persona no identificada, que engañó a la ofendida y se apropió de sus claves electrónicas y realizó los distintos depósitos descritos. Se observa a folio 341 a 342 de la sentencia, los hechos se tuvieron prácticamente por probados, salvo por un aspecto fundamental, el elemento subjetivo doloso (conocimiento y voluntad) de los acusados para la comisión del tipo penal de la estafa informática. Sobre el tema se expuso: "La Representación Fiscal circunscribió la responsabilidad de los imputados al hecho de facilitar las cuentas bancarias para recibir dineros provenientes fraudulentamente de la cuenta de la ofendida, asegurando que los imputados conocían el origen ilegítimo de este dinero, sin que demostrara con prueba idónea y suficiente tal afirmación que es indispensable como elemento subjetivo del tipo penal acusado, el sólo facilitar las cuentas bancaria por parte de los imputados no implica que éstos conocieran de la ideación, planeamiento y ejecución del tipo objetivo que un tercero hubiese realizado para perjudicar el patrimonio de la ofendida a través de medios electrónicos como fue acusado. El Fiscal señaló que los imputados de acuerdo al contrato de apertura de cuenta con la institución bancaria, se les prohíbe facilitar las cuentas a terceros y que incumplieron con tal obligación al facilitar las mismas y formar parte de una organización criminal con un fin común afectando el patrimonio de la ofendida. Sin embargo, el hecho atribuido a los imputados no fue así acusado, aceptar esa modificación en la pieza acusatoria sería una vulneración al principio de correlación entre acusación y sentencia, además el manejo inadecuado de una cuenta bancaria puede conllevar al cierre de la cuenta por la Institución Bancaria al constatar la irregularidad, pero no a una sanción penal, sino a una consecuencia administrativa surgida eventualmente del contrato entre el Banco y el cliente. En cuanto a la declaración rendida por [Nombre 022] y Esteban Obando Ramos, la primera empleada del Banco Nacional de Costa Rica, Sucursal de San Francisco de Dos Ríos y el segundo oficial de la Policía Judicial, ambos son testigos de referencia, cuyos testimonios pese a ser creíbles para este Tribunal, pues se apoyan en lo que percibieron y fue documentado en el Informe Policial 264CI-17 de fecha 16 de mayo de 2017 visible a folio 9 a 17, así como el Informe 465-IP-SITE- 2016 de fecha 01 de julio de 2016 de folio 32 a 35, ninguno de ellos conoció quién realizó las transferencias electrónicas para que el dinero de la cuenta origen propiedad de la ofendida fuera depositado en la cuenta destino de acuerdo a los montos citados a cada uno de los imputados, menos aún si los imputados conocieron o no la manipulación de esta información y el fraude que fue tejido para perjudicar el patrimonio de la ofendida. Se desprende de ambos informe que la investigación surge ante la sospecha de la testigo [Nombre 022] de la Sucursal de San Francisco del Banco Nacional de Costa Rica, que fue la persona que atendió a [Nombre 011] en ese lugar el día 1 de julio de 2016 cuando pretendía retirar de su cuenta dinero, Ericka Alvarado manifestó que por la vestimenta del sujeto y por su experiencia alertó a su superior de un posible fraude, revisando los movimientos en la cuenta corriente registrada a nombre de la ofendida y a su vez se comunicó con la señora [Nombre 001] para que tomara las acciones legales necesaria. La investigación policial en esa agencia bancaria estuvo a cargo de José Zuñiga Campos y de Gabriela Fonseca Vindas, ninguno de estos oficiales fue ofrecido como testigo en esta causa. Por su parte el oficial Esteban Obando Ramos que fue quien compareció al debate, fue claro que tuvo conocimiento de este hecho inicialmente, pero los oficiales citados fueron los que se encargaron de la investigación por ser los designados por la Unidad de Fraudes de San José. Las transferencias electrónicas de la cuenta origen registradas a nombre de la ofendida a las cuentas destino de cada uno de los imputados quedaron documentadas en los citados informes y con la documentación secuestrada producto del levantamiento de secreto bancario ordenado por la Autoridad Jurisdiccional visibles a folio 36 a 37, 38, 42, 92 a 169, que reflejan el ingreso del dinero proveniente de la cuenta de la ofendida a cada una de las cuentas respectivas registrada a nombre de cada imputado por los montos que fueron supracitados, pero esa documentación por más sugestiva que resulta ser no es conclusiva para sostener que los imputados conocían el origen fraudulento de este dinero o que cometieron alguna de las acciones típicas necesarias para la consumación de la Estafa Informática que se les ha venido atribuyendo. La investigación realizada fue endeble a criterio de esta Cámara, de ella no se desprende que los imputados contaran con antecedentes policiales semejantes al hecho acusado, como personas reconocidas como frenteadores o integrantes de una estructura criminal como lo argumentó el señor Fiscal en sus conclusiones. No existió un estudio del perfil de vida de los imputados, es decir, su situación

socioeconómica anterior a este hecho y tampoco después de éste, únicamente se tuvo como cierto los movimientos o transferencia bancarias reportadas por la denunciante como fraudulentas, tampoco se indagó el origen del IP de donde se realizó la transferencia denunciada como fraudulenta. La investigación en síntesis se centró en la verificación de las transferencias únicamente y en el retiro que realizara la imputada [Nombre 009] de la suma de un millón novecientos cincuenta mil colones de su cuenta bancaria, más allá de este hecho no se indagó, aun cuando la ofendida aportó información útil relativa al número telefónico registrado en su celular el día de los hechos, que correspondía a la conversación que fue fundamental para este fraude electrónico que fue víctima. Así las cosas, existiendo una duda razonable sobre la responsabilidad penal de los acusados en aplicación del principio universal in dubio pro reo..."(cfr. folio 347 a 349 de la sentencia. La negrita se suple, la transcripción es literal). Los argumentos esgrimidos se comparten. No existió un error en cuanto al hecho descrito en el punto cuarto de la acusación, debido a que, como se fundamentó, no fue posible determinar el dolo del imputado [Nombre 011] al presentarse a la sucursal del Banco Nacional de Costa Rica, en San Francisco de Dos Ríos. Si bien resultó llamativo el indicio de que el sindicado se presentara en un plazo muy breve en relación con el depósito que se le realizó, y ello, sirvió para alertar a la funcionaria bancaria, ese elemento no es suficiente para poder acreditar el conocimiento por parte del acusado de la estafa informática que se le realizó a la víctima, por lo que la aplicación del principio universal de la duda razonable fue correcta. Misma situación acontece, con el argumento de que el tribunal no adecuó correctamente la participación de los implicados al delito imputado, por la existencia de una coautoría en aplicación de la teoría funcional del hecho. De conformidad con el artículo 45 del Código Penal, son coautores quienes realicen el hecho punible tipificado conjuntamente con el autor. Ello implica conforme a la teoría del dominio funcional del hecho, expuesta por el recurrente, que se cumplan con tres requisitos, según el profesor Roxin: i.- El requisito objetivo, que es la distribución de funciones, donde el aporte debe ser tan importante, de forma que, al hacer una supresión hipotética, el hecho no se hubiera podido cometer sin él. ii. El requisito subjetivo, que es el plan previo. iii. El requisito negativo, que no sea un delito especial propio, culposo, de omisión o de propia mano. Expuesto lo anterior, la tesis fiscal no puede aceptarse, en primer lugar, porque la acusación no describe la coautoría, ni sus elementos, y como segunda limitación, como se expuso en la sentencia, no existen pruebas ni indiciarias o directas, de la existencia de un plan o acuerdo previo, entre los participantes. Por lo que el indicio de una posible distribución de funciones, donde los encartados prestaron sus cuentas para la comisión del delito de estafa informática es insuficiente, en el caso no fue posible siquiera ligar a los acusados (frenteadores) entre sí, y mucho menos, se ofreció prueba sobre la persona que realizó los actos de engaño y apropiación de las claves y realizó las transferencias y su relación con ellos. Esa ausencia de material probatorio idóneo, es la que genera la duda razonable, que fue aplicada al caso en concreto. Sobre las condiciones del acusado [Nombre 011], en el sentido que la cuenta fue de reciente apertura en la relación con los hechos delictivos, que recibió dinero de una persona a quien no conocía ni tenía derecho a recibirlo y su puntualidad de presentación a la entidad financiera, si bien son indicios, no son unívocos, y los mismos son insuficientes, por más referencia que se haga a los informes policiales, o la funcionaria del banco que lo atendió, lo cierto es que no es posible acreditar más allá de toda duda razonable, con la certeza positiva requerida, que el encartado tenía conocimiento del delito que se estaba cometiendo y que formaba parte de un plan de autor. Tampoco es cierto que la prueba bancaria se valoró en forma incorrecta. Como se informa en el fallo, esos elementos sugieren la participación de los acusados en los hechos, pero hasta ahí, en el caso concreto, para poder determinar su responsabilidad penal, era necesario otros indicios o pruebas directas, para considerarlos coautores. La fiscalía pretende que, por la circunstancia de que a los implicados se les depositó el dinero en sus cuentas, y ellos en forma independiente, realizaron pagos, retiros, o se presentaron al banco, sea suficiente para estimar el conocimiento y voluntad en el delito de estafa informática, pero, como se dijo, eso un indicio único. Por ello la afirmación del a quo de la necesidad de contar, con antecedentes policiales o algún otro insumo, como el perfil de vida de los endilgados, para poder concluir la existencia del dolo requerido para la comisión del ilícito, no es errónea. En virtud de lo anterior, la resolución cumple con los requisitos de argumentación de conformidad con el numeral 142 del Código Procesal Penal y respeta las reglas de la sana crítica racional. En consecuencia, los alegatos se deben rechazar. 2) Voto de la jueza Vargas González. Estimo que la impugnación debe ser declarada sin lugar, no por ausencia de indicios para demostrar el dolo de los imputados, sino porque la acusación formulada por el órgano requirente no contiene los elementos necesarios para atribuir a estos una coautoría en el delito de estafa informática. El Ministerio Público acusó lo siguiente: ""“1. Previo a los hechos que se indicarán una persona hasta el momento sin identificar, contactó a los acusados [Nombre 011], [Nombre 009], [Nombre 007] y [Nombre 012], a fin de que le facilitaran el número de su cuenta bancaria, para así utilizar esas cuentas como cuentas receptoras de los dineros que se enviarían haciendo uso

abusivo y no autorizado de los datos que ilegítimamente una persona obtendría de la cuenta bancaria del Banco Nacional de la ofendida [Nombre 001]. Los acusados accedieron a la petición de la persona de calidades desconocidas y le facilitaron a este los números de sus cuentas bancarias. 2. El 01 de julio del 2016, a eso de las 10:00 horas aproximadamente, la ofendida [Nombre 001], recibió una llamada de una persona de identidad desconocida, quien indicó estar interesado en comprar varios muebles que la ofendida tenía a la venta en la página OLX. El sujeto le dijo a la ofendida que el pago de los muebles debía realizarse por medio de una transferencia SINPE, que para realizarla debía hacer una teleconferencia con un supuesto funcionario del Banco Nacional de Costa Rica; en ese instante, se introdujo en la llamada un segundo sujeto, quien antecedido de la música publicitaria del Banco Nacional de Costa Rica indicó ser funcionario de dicho Banco y que en ese momento se enlazaba a la conversación telefónica, para realizar la transferencia de dinero para el pago de los muebles, cuestión falsa pues lo que pretendían esos sujetos era obtener los datos que utiliza la ofendida para accesar a su cuenta y realizar transferencias electrónicas. 3. Para darle confianza a la ofendida, el supuesto funcionario del banco le pidió varios datos al sujeto de calidades desconocidas, tales como los datos de sus tarjetas, el PIN, datos que sujeto le proporcionó. Luego el supuesto funcionario del banco le pidió a la ofendida iguales datos, pero como la ofendida no poseía la clave del cajero el sujeto le pidió las claves para accesar sus cuentas por internet, cuestión a la que accedió la ofendida 4. De forma simultánea mientras la ofendida hablaba con los sujetos conforme le proporcionaba el número de identificación así como de la contraseña de acceso a sus cuentas bancarias, el supuesto funcionario del banco, incidió en el procesamiento de datos del sistema informático del banco de Nacional de Costa Rica, ya que utilizando abusivamente los datos de los que se impuso ilícitamente, acceso a la cuenta en dólares [Valor 002] y colones [Valor 003] del Banco Nacional de Costa Rica propiedad de [Nombre 024] cuya autorizada es la ofendida [Nombre 001] y realizó cuatro transferencias electrónicas por internet banking: por la suma de $5.078.49 dólares (equivalente de ¢2.750.000 millones de colones) hacia la cuenta [Valor 001] del Banco Nacional de Costa Rica, cuyo titular es el imputado [Nombre 011], por la suma de $3.693.44 dólares (equivalente de ¢2.000.000 millones de colones) hacia la cuenta [Valor 004] del Banco Nacional de Costa Rica, cuyo titular es la imputada [Nombre 007], por la suma de $4.616.81 dólares, (equivalente de ¢2.500.000 millones de colones) hacia la cuenta [Valor 005] del Banco Nacional de Costa Rica, cuyo titular es el imputado [Nombre 012], a las 11:14 horas aproximadamente, por la suma de ¢950.000 y ¢1.000.000 de colones hacia la cuenta 10000015201000151 del Banco Nacional de Costa Rica, cuyo titular es la imputada [Nombre 009]. 5. Una vez acreditados los fondos en las cuentas de los acusados, ese mismo día, los imputados conociendo el origen ilegítimo de dinero, hicieron el retiro de los dineros transferidos, en el caso de la acusada [Nombre 009], al ser las 11:49 horas aproximadamente, se apersonó a la ventanilla de la Agencia del Banco de Costa Rica, oficina 377, ubicado en San José y retiró la suma de ¢1.500.000 millones de colones, de seguido ese mismo día, al ser las 11:55 horas en el cajero automático del mismo banco, retiró en dos tractos la suma de ¢250.000 y ¢200.000 colones. Asimismo, el acusado [Nombre 011], se apersonó a la ventanilla de la agencia del Banco Nacional de Costa Rica, en San Francisco de dos Ríos gestionó el retiro de los dineros transferidos ilícitamente, sin embargo, el banco detectó de fraude y bloqueó la cuenta del acusado, siendo detenido en el sitio. Del mismo modo el acusado [Nombre 012], se apersonó a la ventanilla del Banco Nacional de Costa Rica, oficinas Centrales en San José, gestionó el retiro de los dineros transferidos ilícitamente, sin embargo el banco detectó el fraude y bloqueó la cuenta del acusado, siendo detenido en el sitio y la imputada [Nombre 007] se apersonó a la ventanilla del Banco Nacional de Costa Rica, en Heredia, gestionó el retiro de los dineros transferidos ilícitamente, sin embargo el banco detectó el fraude y bloqueó la cuenta de la acusado." (cfr. acusación de folio 170 a 172, el destacado no es del original). Como se observa, el Ministerio Público atribuyó a los justiciables [Nombre 011], [Nombre 009], [Nombre 007] y [Nombre 012]: i) facilitar sus cuentas para usarlas como receptoras del dinero que se enviaría haciendo “uso abusivo y no autorizado” de datos que, de forma ilegítima, se obtendrían de la cuenta de la ofendida [Nombre 001]; y ii) retirar los fondos a pesar de que conocían su origen ilegítimo. Como se ve, en ningún momento se imputó a los endilgados ser parte de un grupo criminal dedicado a la ejecución de estafas informáticas, o, cuando menos, actuar con una resolución o plan común en el caso concreto, único contexto en el cual la conducta de un coautor (y que, en realidad, es solo una contribución dentro del plan adoptado) se le puede imputar a otro. Se insiste, nunca se indicó que [Nombre 011], [Nombre 009], [Nombre 007] y [Nombre 012] actuasen de común acuerdo con quien, usando indebidamente los datos que obtuvo vía telefónica de la víctima, manipuló el ingreso y procesamiento de esos datos en el sistema informático del Banco Nacional de Costa Rica y trasladó dinero de la cuenta de [Nombre 001] a las de los primeros, de donde la conducta de esa persona cuya identidad, a la fecha, se desconoce, no podría imputárseles a quienes, según la acusación, se limitaron a facilitar sus cuentas para recibir un dinero que

se les enviaría haciendo un “uso abusivo de datos” (que no se especifica en qué consiste) y a retirarlo. Conviene hacer notar que, solo añadiendo aspectos que la requisitoria no contiene, se podría concluir que existió un plan común, donde quienes prestaban sus cuentas y retiraban los dineros sabían que otro u otros sujetos procedían al despojo del dinero en los términos que apuntan los hechos 2.-, 3.- y 4.- de la acusación (que no son, sino, los del tipo penal de la estafa informática). En este contexto, donde la imputación no contiene la información necesaria para establecer una coautoría, estimo que los reclamos que formula el recurrente deben declararse sin lugar, ya que incluso admitiendo hipotéticamente que hay indicios para establecer que los endilgados actuaron dolosamente, y que no fue por azar o casualidad que recibieron y retiraron el dinero transferido desde la cuenta de la víctima, era inviable el dictado de una condena. Por lo dicho, los alegatos deben rechazarse. IV.- Voto salvado de la jueza Montero Mena: Respeto profundamente el criterio de mi compañera Jueza y Juez; sin embargo, razones de orden jurídico me hacen apartarme del voto de mayoría por siguiente: En el sub júdice, puede observarse que la acusación presentada por el Ministerio Público refirió: “1. Previo a los hechos que se indicarán una persona hasta el momento sin identificar, contactó a los acusados [Nombre 011], [Nombre 009], [Nombre 007] y [Nombre 012], a fin de que le facilitaran el número de su cuenta bancaria, para así utilizar esas cuentas como cuentas receptoras de los dineros que se enviarían haciendo uso abusivo y no autorizado de los datos que ilegítimamente una persona obtendría de la cuenta bancaria del Banco Nacional de la ofendida [Nombre 001]. Los acusados accedieron a la petición de la persona de calidades desconocidas y le facilitaron a este los números de sus cuentas bancarias. 2. El 01 de julio del 2016, a eso de las 10:00 horas aproximadamente, la ofendida [Nombre 001], recibió una llamada de una persona de identidad desconocida, quien indicó estar interesado en comprar varios muebles que la ofendida tenía a la venta en la página OLX. El sujeto le dijo a la ofendida que el pago de los muebles debía realizarse por medio de una transferencia SINPE, que para realizarla debía hacer una teleconferencia con un supuesto funcionario del Banco Nacional de Costa Rica; en ese instante, se introdujo en la llamada un segundo sujeto, quien antecedido de la música publicitaria del Banco Nacional de Costa Rica indicó ser funcionario de dicho Banco y que en ese momento se enlazaba a la conversación telefónica, para realizar la transferencia de dinero para el pago de los muebles, cuestión falsa pues lo que pretendían esos sujetos era obtener los datos que utiliza la ofendida para accesar a su cuenta y realizar transferencias electrónicas. 3. Para darle confianza a la ofendida, el supuesto funcionario del banco le pidió varios datos al sujeto de calidades desconocidas, tales como los datos de sus tarjetas, el PIN, datos que sujeto le proporcionó. Luego el supuesto funcionario del banco le pidió a la ofendida iguales datos, pero como la ofendida no poseía la clave del cajero el sujeto le pidió las claves para accesar sus cuentas por internet, cuestión a la que accedió la ofendida 4. De forma simultánea mientras la ofendida hablaba con los sujetos conforme le proporcionaba el número de identificación así como de la contraseña de acceso a sus cuentas bancarias, el supuesto funcionario del banco, incidió en el procesamiento de datos del sistema informático del banco de Nacional de Costa Rica, ya que utilizando abusivamente los datos de los que se impuso ilícitamente, acceso a la cuenta en dólares [Valor 002] y colones [Valor 003] del Banco Nacional de Costa Rica propiedad de [Nombre 024] cuya autorizada es la ofendida [Nombre 001] y realizó cuatro transferencias electrónicas por internet banking: por la suma de $5.078.49 dólares (equivalente de ¢2.750.000 millones de colones) hacia la cuenta [Valor 001] del Banco Nacional de Costa Rica, cuyo titular es el imputado [Nombre 011], por la suma de $3.693.44 dólares (equivalente de ¢2.000.000 millones de colones) hacia la cuenta [Valor 004] del Banco Nacional de Costa Rica, cuyo titular es la imputada [Nombre 007], por la suma de $4.616.81 dólares, (equivalente de ¢2.500.000 millones de colones) hacia la cuenta [Valor 005] del Banco Nacional de Costa Rica, cuyo titular es el imputado [Nombre 012], a las 11:14 horas aproximadamente, por la suma de ¢950.000 y ¢1.000.000 de colones hacia la cuenta 10000015201000151 del Banco Nacional de Costa Rica, cuyo titular es la imputada [Nombre 009]. 5. Una vez acreditados los fondos en las cuentas de los acusados, ese mismo día, los imputados conociendo el origen ilegítimo de dinero, hicieron el retiro de los dineros transferidos, en el caso de la acusada [Nombre 009], al ser las 11:49 horas aproximadamente, se apersonó a la ventanilla de la Agencia del Banco de Costa Rica, oficina 377, ubicado en San José y retiró la suma de ¢1.500.000 millones de colones, de seguido ese mismo día, al ser las 11:55 horas en el cajero automático del mismo banco, retiró en dos tractos la suma de ¢250.000 y ¢200.000 colones. Asimismo, el acusado [Nombre 011], se apersonó a la ventanilla de la agencia del Banco Nacional de Costa Rica, en San Francisco de dos Ríos gestionó el retiro de los dineros transferidos ilícitamente, sin embargo, el banco detectó de fraude y bloqueó la cuenta del acusado, siendo detenido en el sitio. Del mismo modo el acusado [Nombre 012], se apersonó a la ventanilla del Banco Nacional de Costa Rica, oficinas Centrales en San José, gestionó el retiro de los dineros transferidos ilícitamente, sin embargo el banco detectó el fraude y bloqueó la cuenta del acusado, siendo detenido en el sitio y la imputada [Nombre 007] se

apersonó a la ventanilla del Banco Nacional de Costa Rica, en Heredia, gestionó el retiro de los dineros transferidos ilícitamente, sin embargo el banco detectó el fraude y bloqueó la cuenta de la acusado." (Cfr. acusación de folio 170 a 172). La representación fiscal aduce que el fallo se fundó en una errónea determinación de los hechos probados, específicamente en el punto cuarto, donde el tribunal de mérito tiene como probado que el acusado [Nombre 011] se apersonó a la ventanilla de la agencia del Banco Nacional de Costa Rica, en San Francisco de Dos Ríos, lugar donde fue detenido, pero que se omitió tener por demostrado que el sindicado se presentó y solicitó el retiro de los fondos que le habían sido transferidos a su cuenta bancaria instantes previos, lo anterior a pesar de que efectivamente se pudo corroborar la presencia del justiciable en la entidad bancaria a efectos de poder sacar el dinero que previamente había sido depositado en la cuenta que este había aperturado a su nombre. Tal y como se desprende de la anterior transcripción, la pieza acusatoria, imputó a todos los implicados ([Nombre 011], [Nombre 012], [Nombre 009] y [Nombre 007], del delito de estafa informática), así se acusó, por ejemplo, que [Nombre 011], facilitó su cuenta bancaria a sujetos desconocidos, para que fuera utilizada como receptora de los dineros que iban a ser despojados fraudulentamente a la ofendida [Nombre 001]. Tal y como lo afirmó quien impugna, en el caso de [Nombre 011], mediante el informe policial 465-IP-SITE-2016 de la Sección de Investigaciones de Turno Extraordinario, se demostró que su presencia en la entidad bancaria, la cual fue inmediata en relación con la transferencia, aspecto que se logró establecer con la declaración de la testigo [Nombre 022]. En consecuencia, estima esta juzgadora que la pieza acusatoria, es clara, precisa y circunstanciada en torno a la conducta que se le imputó a los encausados y concretamente en el caso de Andy, el hecho cuarto de la pieza acusatoria es claro. Además, estimo que, la duda no ha sido debidamente fundada, pues el análisis de la prueba debe ser armónico y conjunto, tanto así que, la sentencia debe basarse a sí misma y debe reflejar una ponderación adecuada de la pruebe directa, así como la indiciaria, cirunstancia que no se observa en el caso de [Nombre 011], así como de los demás encausados a saber: [Nombre 012], [Nombre 009] y [Nombre 007], de ahí la deficiencia que presenta la sentencia venida en alzada. Además, estimo que, debió analizarse a profundidad porque las acusadas no se adecúan al delito de estafa informática previsto y sancionado en el artículo 217 bis del Código Penal, máxime que, debe considerarse que este tipo de delincuencia a ser novedosa en nuestro sistema de justicia penal, requiere que las personas juzgadoras realicen un análisis comprensivo, amplio y bien ponderado de todas las actuaciones realizadas por el autor o autores. Consecuentemente se debió razonar si la determinación de la acción -realizar una llamada de teléfono a la víctima con la finalidad de lograr mediante el ardid dispuesto que esta facilitara sus números de cuenta y claves de acceso- para que, una vez que los autores del hecho entraron en poder de esos mecanismos de seguridad se dispusieran mediante el uso de herramientas tecnológicas, -como lo son los sistemas informáticos- a realizar las transferencias de dinero a cuentas propiedad de los encausados. Ciertamente el fallo es omiso en analizar esos aspecto y, por ende se denota una falta de análisis de la figura de coautoría, donde los intervinientes por medio del dominio funcional del hecho deciden llevar a adelante una acción y ejecutarla; nótese que los encausados, no solamente desempeñaron un papel en el despliegue de la acción –aperturando y facilitando sus cuentas- sino que intentaron consumar el hecho al momento de tratar de retirar el dinero que había sido depositado por parte de la autorizada de [Nombre 024 001] mediante transferencias electrónicas por internet banking: nótese que en caso de [Nombre 011] el depósito se realizó por la suma de $5.078.49 dólares (equivalente de ¢2.750.000 millones de colones) hacia la cuenta [Valor 001] del Banco Nacional de Costa Rica, cuyo titular lo es el imputado. En razón de lo anterior, debe darse razón a quien impugna, pues efectivamente en el fallo se observa un déficit argumentativo en torno a la figura de la coautoría del delito de estafa en su modalidad informática, pues, aunque no se haya demostrado que los sindicados hayan realizado las llamadas a las víctimas o, realizado las transferencias desde la cuenta de la ofendida hacia las suyas, se debía analizar la escencialidad de su participación y sobre todo si su actuación obedeció a un dolo directo, así como sí conocían el origen fraudulento de este dinero, o bien si existía alguna justificación para que consideraran que una transferencia a sus cuentas por altas sumas de dinero estaba justificada. Por otra parte, no comparte esta juzgadora el criterio del a quo en el sentido de que la investigación realizada fue endeble y que los imputados no contaban con antecedentes policiales semejantes al hecho acusado, o bien fueran reconocidas como frenteadores o integrantes de una estructura criminal, pues, esa es conclusión falaz, en el tanto no es necesario que una persona figure en los archivos policiales o que haya sido investigada previamente para que pueda cometer un ilícito como el que se investigó. En razón de lo anterior y por estimar que la duda no ha sido debidamente fundada, además de que se denota un déficit en el análisis de la tipicidad de la conducta acusada, voto por anular el fallo y ordenar el juicio de reenvío para nueva sustanciación conforme a derecho.

POR TANTO:

Por mayoría, se declara sin lugar el recurso de apelación interpuesto por el licenciado Carlos Castro Sojo, en representación del Ministerio Público. La jueza Montero Mena salva el voto. NOTIFÍQUESE.

Gustavo Adolfo Rojas Gutiérrez

Patricia Vargas González Elizabeth Montero Mena Juez y juezas de Apelación de Sentencia Penal

Expediente: 16-003520-0059-PE (14)
Imputado: [Nombre 011] y otros
Ofendida: [Nombre 001]
Delito: Estafa informática

lquirosg

Resolución N° 01076-2020 Sala Tercera

Sala Tercera de la Corte

Resolución Nª 01076 - 2020

Fecha de la Resolución: 28 de agosto del 2020
Expediente: 13-001603-0042-PE
Redactado por: Álvaro Burgos Mata
Clase de Asunto: Recurso de casación
Analizado por: SALA DE CASACIÓN PENAL
Indicadores de Relevancia
Sentencia Relevante

Sentencias del mismo expediente

Sentencia con datos protegidos, de conformidad con la normativa vigente

Contenido de Interés:
Temas (descriptores): Estafa informática
Subtemas (restrictores): Bien jurídico tutelado
Tipo de contenido: Voto de mayoría
Rama del derecho: Penal

III. (...). Para arribar a esta conclusión, se debe partir de la configuración misma del tipo penal de estafa informática que está regulado en el artículo 217 bis del Código Penal: “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”. En la estafa informática el bien jurídico tutelado es el patrimonio, razón por la que la actividad fraudulenta del agente se relaciona con la manipulación del sistema informático para obtener un beneficio patrimonial antijurídico, de ahí que la utilización del cajero automático dándole órdenes para que dispensara tractos de dinero específicos y la tarjeta de crédito copiada que se utilizó para intentar pagar por bienes mediante transacciones que resultaron denegadas, son el medio empleado por los imputados para alcanzar su finalidad delictiva de lesionar el patrimonio ajeno. Por otro lado, la estructura del tipo penal, hace alusión precisamente a la utilización de datos falsos para incidir en el procesamiento de los mismos por parte del sistema y lograr así el beneficio patrimonial indebido, y esto es precisamente lo que hacen los encartados. (...).
... Ver menos

Citas de Legislación y Doctrina Sentencias Relacionadas

Contenido de Interés:
Temas (descriptores): Estafa informática
Subtemas (restrictores): Concurso material
Tipo de contenido: Voto de mayoría
Rama del derecho: Penal

III. (...). En el caso de Sáenz Méndez, queda claro de la lectura del cuadro fáctico acusado y tenido por demostrado, que la encartada realizó en cada uno de esos días, 08 y 09 de enero del 2013 respectivamente, una serie de acciones materiales que versaron en la utilización de la misma tarjeta falsa, sea la 4152 7611 5892 9120, con la que logró influir en el procesamiento de datos del mismo sistema informático del cajero automático del emisor de la tarjeta al que le dio órdenes de dispensa de dinero consecutivas que se producen como parte de un solo acto y persiguiendo la misma finalidad, ejecutadas de forma cercana en el tiempo y en el mismo espacio, de manera inmediata (con aproximadamente un minuto de diferencia entre una y otra), con identidad de sujeto pasivo y sujeto activo, por lo que constituyen una única acción en sentido jurídico penal, ya que denotan una sola resolución criminal, que no está interrumpida por factor alguno que evidenciara el cese en sentido estricto de la acción típica. La descripción fáctica de los hechos probados en torno a lo sucedido los días 8 y 9 de enero del 2013, no permite acreditar entonces, la existencia de acciones independientes que agoten cada una de ellas el tipo penal de la estafa informática, como lo pretende la recurrente. Así las cosas, en el presente caso, a partir de los hechos que se tuvieron por acreditados en sentencia de primera instancia, se determina que las conclusiones a las que arribó el
ad quem son correctas y, por ende, las acciones descritas como cometidas por la imputada Sáenz Méndez se deben tener como
constitutivas de un delito de estafa informática cometido el 8 de enero del 2013 y un delito de estafa informática cometido el 9 de enero del 2013. Es importante, dejar en claro en este punto que a criterio del ad quem en el fallo recurrido, las acciones desplegadas por Sáenz Méndez los días 08 y 09 de enero del 2013, concursan entre sí materialmente, lo que no fue objeto de impugnación y no se entra a valorar en esta sede porque precisamente se dispone que en el juicio de reenvío deben aplicarse las reglas del delito continuado, respetando el principio de no reforma en perjuicio, de manera tal que este aspecto en particular no tiene incidencia en la pena a imponer en el caso concreto puesto que habiéndose determinado que entre lo sucedido en ambos días no hay una unidad de acción se descarta el concurso ideal y por ende, resulta ser más beneficioso para la encartada el que se apliquen las reglas de fijación de pena de conformidad con lo establecido en el artículo 77 del Código Penal, que las correspondientes al concurso material de delitos, según se establece en el numeral 76 del mismo cuerpo normativo.(...).
... Ver menos

Citas de Legislación y Doctrina Sentencias Relacionadas

Texto de la Resolución

130016030042PE

Exp: 13-001603-0042-PE Res:
2020-01076

SALA DE CASACIÓN PENAL. San José, a las trece horas y veinticinco minutos del veintiocho de agosto de dos mil veinte.

Recurso de Casación, interpuesto en la presente causa seguida contra César Francisco González Paéz, mayor, costarricense, cédula de identidad número 1-0768-0350, nacido en San José, el 30 de enero de 1970, hijo de César González Pérez y Sonia Páez Zúñiga, casado, de oficio chofer, Glenda Lisseth Sáenz Méndez, mayor, nicaragüense, documento de identidad número 15807892702, nacida en Nicaragua, el 09 de febrero de 1986, hija de Tomás Méndez y Francisca Sáenz, soltera, de oficio operaria de fábrica, Roberto Ortiz Finalet, mayor, cubano, documento de identidad número 119200274212, nacido en Cuba, el 02 de mayo de 1954, hijo de Tomás Ortiz de la Cruz y Celia Finalet Hernández, soltero, de oficio ebanista, Donald Mauricio Ureña Hernández, mayor, costarricense, cédula de identidad número 1-0932-0814, nacido en San José, el 13 de marzo de 1976, hijo de Elizabeth Hernández Peñaranda, soltero, de oficio taxista informal y Alejandro Papadopolo Moya, mayor, costarricense, cédula de identidad número 1-1094-0981, nacido en San José, el 25 de febrero de 1981, hijo de Wallace Papadopolo Baily y Marianela Moya Quesada, soltero, de oficio decorador de interiores; por el delito de estafa informática, cometido en perjuicio de Banco de Costa Rica y otros. Intervienen en la decisión del recurso, los Magistrados y Magistradas Patricia Solano Castro, Álvaro Burgos Mata, Gerardo Rubén Alfaro Vargas, Sandra Eugenia Zúñiga Morales y Ronald Cortés Coto, este último como Magistrado suplente. Además, en esta instancia, la licenciada Ruth María Quesada Quesada, como representante del Ministerio Público.

Resultando:

1. Mediante sentencia N° 2019-1945, dictada a las once horas y veinte minutos del treinta de octubre de dos mil diecinueve, el Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José, resolvió: “POR TANTO: Se declara sin lugar el recurso de apelación interpuesto por el imputado César González Páez. Se declara parcialmente con lugar, aunque por razones distintas de las expuestas por el defensor, el recurso de apelación interpuesto por el licenciado Jorge Vallejo Alfaro, en favor del imputado Alejandro Papadopolo Moya y en consecuencia, se anula la sentencia respecto de la condenatoria dispuesta contra este imputado por los hechos atribuidos del 31 de enero del 2013. Se mantiene la condenatoria dispuesta contra este imputado, por los hechos delictivos cometidos el 29 de enero del 2013 en el establecimiento comericial IESA y respecto de estos se revoca la calificación jurídica dada a los mismos en la sentencia de instancia y en su lugar se dispone recalificarlos como dos delitos de estafa informática en concurso ideal. Se ordena el reenvío a juicio para una nueva sustanciación de los extremos anulados y para la imposición de la pena correspondiente. Por razones distintas de las alegadas por la defensa, se declara parcialmente con lugar el recurso de apelación interpuesto por el licenciado Gilberto Corella Quesada, en favor de la imputada Glenda Lisseth Sáenz Méndez. Se anula la sentencia en cuanto dispuso la condenatoria de la imputada por los hechos que le atribuyen haber efectuado cuatro retiros de efectivo del cajero automático del Citi Bank de Santa Ana el día 9 de enero del 2013 y se ordena el reenvío a juicio para una nueva sustanciación de los mismos. Se mantiene la condenatoria dispuesta contra la imputada por los hechos que le atribuyen haber efectuado tres retiros de efectivo el día 8 de enero del 2013 en el cajero automático de Citi Bank, Santa Ana y dos retiros de efectivo del cajero automático del Fresh Market, Santa Ana, el 9 de enero del 2013. Se revoca la calificación jurídica que se dio en sentencia a esos hechos y se ordena recalificarlos como un delito de estafa informática cometido el 8 de enero del 2013 y un delito de estafa informática cometido el 9 de enero del 2013, concurrentes materialmente, pero a los que ha de aplicarse la penalidad del delito continuado, en aplicación del principio de no reforma en perjuicio. Para la determinación de la pena, conforme estos parámetros se ordena el reenvío a juicio. Por razones distintas de las alegadas, se declara parcialmente con lugar el recurso de apelación interpuesto por la defensora pública Gaudy Quesada Rodríguez, en favor del imputado Donald Ureña Hernández. Se anula la sentencia de instancia en cuanto le condena como coautor de los hechos delictivos atribuidos a

Alejandro Papadopolo Moya, el 31 de enero del 2013 y de los retiros de efectivo realizados por Glenda Sáenz Méndez, el día 9 de enero del 2013 en el cajero automático del Citi Bank, Santa Ana y en relación con este conjunto fáctico, el reenvío a juicio ordenado deberá comprender también la determinación de responsabilidad del imputado Ureña Hernández. Se mantiene la condenatoria del justiciable, dispuesta en relación con los delitos de estafa informática cometidos en coautoría con Alejandro Papadopolo Moya el 29 de enero del 2013 y con Glenda Sáenz Méndez el 8 y 9 de enero. En relación con estos hechos, se revoca su calificación jurídica y se dispone su recalificación, determinándose que Ureña Hernández es coautor de dos delitos de estafa informática en concurso

ideal, cometidos el 29 de enero del 2013 que concurren materialmente con un delito de estafa informática cometidos el 08 de enero del 2013 y estos a su vez, en concurso material con un delito de estafa informática cometidos el 9 de enero del 2013, debiendo fijarse la penalidad de los materialmente concurrentes, de

conformidad con las reglas del delito continuado, en aplicación del principio de no reforma en perjuicio. Se ordena el reenvío a juicio para la fijación de la pena correspondiente. Se declara sin lugar el recurso de apelación presentado a título personal por el imputado Donald Ureña Hernández. Se ordena prorrogar por tres meses, contados a partir del 20 de noviembre del 2019 y hasta el 20 de febrero del 2020, la medida cautelar de prisión preventiva que se ha impuesto a los imputados Alejandro Papadopolo Moya, Glenda Lisseth Sáenz Méndez y Donald Ureña Hernández. NOTIFÍQUESE. - Manuel Gómez Delgado Gustavo Gillen Bermúdez Marianela Corrales Pampillo Jueces y jueza de Apelación de Sentencia Penal" (sic).

2. Contra el anterior pronunciamiento, la licenciada Ruth María Quesada Quesada, como representante del Ministerio Público, interpuso recurso de casación.
3. Verificada la deliberación respectiva, la Sala entró a conocer del recurso.
4. En los procedimientos se han observado las prescripciones legales pertinentes. Informa el Magistrado Burgos Mata; y,

Considerando:

I .- Mediante resolución 2020-00166, de las diez horas y cincuenta y cinco minutos del catorce de febrero del dos mil veinte(cfr. folios 843 a 845), esta Sala admitió para su conocimiento de fondo el recurso de casación interpuesto por la licenciada Ruth María Quesada Quesada en representación del Ministerio Público y en contra de la resolución número 2019-1945, de las once y veinte minutos, del treinta de octubre de dos mil diecinueve, dictada por el Tribunal de Apelación de la Sentencia Penal del Segundo Circuito Judicial de San José, Goicoechea , en la que se resolvió: "POR TANTO: Se declara sin lugar el recurso de apelación interpuesto por el imputado César González Páez. Se declara parcialmente con lugar, aunque por razones distintas de las expuestas por el defensor, el recurso de apelación interpuesto por el licenciado Jorge Vallejo Alfaro, en favor del imputado Alejandro Papadopolo Moya y, en consecuencia, se anula la sentencia respecto de la condenatoria dispuesta contra este imputado por los hechos atribuidos del 31 de enero del 2013. Se mantiene la condenatoria dispuesta contra el imputado, por los hechos delictivos cometidos del 29 de enero del 2013 en el establecimiento comercial IESA y respecto de estos se revoca la calificación jurídica dada a los mismos en la sentencia de instancia y en su lugar se dispone recalificarlos como dos delitos de estafa informática en concurso ideal. Se ordena el reenvío a juicio para una nueva sustanciación de los extremos anulados y para la imposición de la pena correspondiente. Por razones distintas de las alegadas por la defensa, se declara parcialmente con lugar el recurso de apelación interpuesto por el licenciado Gilberto Corella Quesada, en favor de la imputada Glenda Lisseth Sáenz Méndez. Se anula la sentencia en cuanto dispuso la condenatoria de la imputada por los hechos que le atribuyen haber efectuado cuatro retiros de efectivo del cajero automático del Citi Bank de Santa Ana el día 9 de enero del 2013 y se ordena el reenvío a juicio para una nueva sustanciación de los mismos. Se mantiene la condenatoria dispuesta contra la imputada por los hechos que le atribuyen haber efectuado tres retiros de efectivo el día 8 de enero del 2013 en el cajero automático de Citi Bank, Santa Ana y dos retiros de efectivo del cajero automático del Fresh Market, Santa Ana, el 9 de enero del 2013. Se revoca la calificación jurídica que se dio en sentencia a esos hechos y se ordena recalificarlos como un delito de estafa informática cometido el 8 de enero del 2013 y un delito de estafa informática cometido el 9 de enero del 2013, concurrentes materialmente, pero a los que ha de aplicarse la penalidad del delito continuado, en aplicación del principio de no reforma en perjuicio. Para la determinación de la pena, conforme estos parámetros se ordena el reenvío a juicio. Por razones distintas de las alegadas, se declara parcialmente con lugar el recurso de apelación interpuesto por la defensora pública Gaudy Quesada Rodríguez, en favor del imputado Donald Ureña Hernández. Se anula la sentencia de instancia en cuanto le condena como coautor de los hechos delictivos atribuidos a Alejandro Papadopolo Moya, el 31 de enero del 2013 y de los retiros en efectivo realizados por Glenda Sáenz Méndez, el día 9 de enero del 2013 en el cajero automático del Citi Bank, Santa Ana y en relación con este conjunto fáctico, el reenvío a juicio ordenado deberá comprender también la determinación de responsabilidad del imputado Ureña Hernández. Se mantiene la condenatoria del justiciable, dispuesta en relación con los delitos de estafa informática cometidos en coautoría con Alejandro Papadopolo Moya el 29 de enero del 2013 y con Glenda Sáenz Méndez el 8 y 9 de enero. En relación con estos hechos, se revoca su calificación jurídica y se dispone su recalificación determinándose que Ureña Hernández es coautor de dos delitos de estafa informática en concurso ideal, cometidos el 29 de enero del 2013 que concurren materialmente con un delito de estafa informática cometidos el 8 de enero del 2013 y estos a su vez, en concurso material con un delito de estafa informática cometidos el 9 de enero del 2013, debiendo fijarse la penalidad de los materialmente concurrentes, de conformidad con las reglas del delito continuado, en aplicación del principio de no reforma en perjuicio. Se ordena el reenvío a juicio para la fijación de la pena correspondiente. Se declara sin lugar el recurso de apelación presentado a título

personal por el imputado Donald Ureña Hernández. Se ordena prorrogar por tres meses, contados a partir del 20 de noviembre del 2019 y hasta el 20 de febrero del 2020, la medida cautelar de prisión preventiva que se ha impuesto a los imputados Alejandro Papadopolo Moya, Glenda Lisseth Sáenz Méndez y Donald Ureña Hernández. Notifíquese" (cfr. folios 777 a 778). II.- Objeto del recurso de Casación. En su único motivo, la representante del Ministerio Público alega la inobservancia del artículo 76 del Código Penal y la errónea aplicación del numeral 75 del mismo cuerpo legal, lo que tiene incidencia directa en la pena impuesta a los acusados Alejandro Papadopolo Moya, Glenda Lisseth Sáenz Méndez y Donald Ureña Hernández. Fundamenta el reproche en el artículo 468, inciso b), del Código Procesal Penal. De seguido, transcribe in extenso la sentencia dictada por el ad quem (cfr. folios 787 vuelto al 789 frente) y arguye que en el caso que nos ocupa es evidente que existieron acciones independientes y no una unidad de acción como se sostuvo en la sentencia impugnada. Alega que en relación con el imputado Papadopolo Moya, el Tribunal de Apelación de Sentencia Penal, recalificó equivocadamente los hechos sucedidos el 29 de enero del 2013 en el local comercial IESA, en Barrio México, con una separación temporal de un minuto (primer evento a las 14:58 y el segundo a las 14:59), a dos delitos de estafa informática en concurso ideal, cuando lo correcto es entender las dos transacciones hechas por esta persona como cometidos en concurso material, puesto que si bien es cierto, la intención del imputado con ambas transacciones lo fue, pagar la compra de materiales eléctricos mediante el uso de una tarjeta falsa, existió entre ellas una separación espacio temporal de un minuto. Sostiene que si bien es cierto se trató de un mismo sistema informático, se afectó o puso en peligro el mismo bien jurídico y se trató de la misma persona ofendida, no se puede concluir que ambos delitos consumados se ejecutaran mediante una única acción y que por ende, se tratara de un concurso ideal de delitos, porque cada delito se configuró desde el momento en que el imputado, a sabiendas de la falsedad de la tarjeta, la utilizó para el pago de la compra, en una primera y en una segunda ocasión, de manera que para cada una de ellas se requirió de la manipulación, el influjo o el mal uso de los datos para procurar el beneficio patrimonial antijurídico, por lo que se consumó el delito de forma homogénea configurándose dos delitos de estafa informática en concurso material a los que debe aplicarse las reglas del delito continuado porque en cada una de las ocasiones se afectó o se puso en peligro un bien jurídico patrimonial, aún y cuando la finalidad en los dos hechos era la misma. Idéntica situación sucede a su criterio, en relación a la imputada Glenda Liseth Sáenz Méndez, para quien el Tribunal de Apelación de Sentencia Penal, recalifica los hechos tenidos por demostrados y concluye que los diferentes retiros de dinero efectuados por ella, tres el 8 de enero del 2013 en el cajero de Citi Bank, Santa Ana, y dos más realizados el 9 de enero del 2013 en el cajero de Fresh Market, Santa Ana, constituyen un único delito y no delitos independientes, como lo concluyó el a quo. A criterio de la impugnante, a pesar de que los diferentes retiros efectuados en la misma fecha derivan de un mismo empleo de datos para la pluralidad de sustracciones de una masa común, diferida por la orden de dispensar en tractos un monto de dinero específico, y de que esto sucedió en un espacio temporal sumamente corto, es equivocado considerar que se trata de un único delito. Considera la fiscal que "tanto en las transacciones comerciales llevadas a cabo por el imputado Papadopolo Moya como en los retiros de los cajeros automáticos efectuados por Glenda Lisseth Sáenz Méndez, la intención del agente activo en cada transacción comercial o en cada retiro, era la procura del pago de una factura o bien el retiro de una determinada cantidad de dinero, dándose una separación espacio temporal entre las ejecuciones, aunque fuese mínima; así mismo, aún y cuando se trató del mismo sistema informático, del mismo bien jurídico, referente a la misma persona ofendida, a pesar de todo ello, no es procedente concluir, que las acciones consumadas, se ejecutaron mediante una única acción y por ende se trata de un concurso ideal de delitos y no uno material, por cuanto cada delito se configuró desde el momento en que el agente activo, a sabiendas de la falsedad de la tarjeta, realizó cada una de las transacciones o cada uno de los retiros de los cajeros" (sic; cfr. folio 790). A continuación, transcribe in extenso, un pronunciamiento del Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José, el cual analiza la naturaleza y los alcances de las reglas del concurso material (cfr. folios 790 frente al 791 frente). Desde su óptica, el a quo no incurrió en yerro alguno al calificar los hechos acusados y acreditados como constitutivos de los delitos de estafa informática en concurso material, en la modalidad de delito continuado, pues dicha fijación se realizó en estricto apego a los artículos 76 y 77 del Código Penal. Concluye reiterando que los hechos acreditados, con respecto a cada uno de los imputados, se dieron de forma independiente, ya fuese en el caso de las transacciones comerciales, o bien, con respecto a los retiros de cajeros automáticos. Subraya que se trata de acciones separadas, las cuales se ejecutan en concurso material homogéneo, a pesar de que se hayan consumado (en algunos de los casos) con una mínima separación espacio temporal, en relación con el mismo sistema informático, lesionando el mismo bien jurídico tutelado, y guiadas por una misma finalidad fraudulenta. Como agravio, aduce que la resolución dictada por el ad quem

lesionó el principio de tutela judicial efectiva, en tanto ocasionó un perjuicio ilegítimo a las pretensiones punitivas del Ministerio Público, quien ha venido sosteniendo a lo largo del proceso, que los hechos en cuestión concursan materialmente. Reprocha que la recalificación que operó en segunda instancia fue arbitraria y ha incidido en la fijación de la pena. Como pretensión solicita se declare con lugar el presente motivo de casación, se revoque la resolución recurrida y se mantenga lo resuelto por el tribunal de juicio.

III.- Aspectos de interés para la resolución del caso: Con el fin de tener claros los antecedentes originarios del presente alegato, se estima necesario hacer referencia, en primer lugar, al marco fáctico que se tuvo por acreditado en la presente causa, respecto a los eventos que resultan de interés para la resolución del motivo admitido para su estudio de fondo. En este sentido, se tuvo por acreditado que: “1) En el período comprendido entre el mes de diciembre del 2012 y febrero del 2013, los acusados DONALD MAURICIO UREÑA HERNÁNDEZ, GLENDA LISETH SANZ, ALEJANDRO PAPADOPOLO MOYA, idearon un
plan con el fin de lograr la obtención de beneficios económicos antijurídicos, dicho plan consistía en la entrar en posesión de tarjetas falsificadas de crédito y débito que serían utilizadas posteriormente para realizar compras y retiros de dinero en diversos comercios del país, siendo que una vez impuestos de la información contenida en las bandas magnéticas de las tarjetas por medio de tarjetas falsificadas que se elaboraban de una forma que no se pudo determinar y las utilizaban en distintos locales comerciales y realizaban retiros en cajeros automáticos. Determinándose que el encartado Donald Mauricio Ureña Hernández, brindaba custodia y transporte en el vehículo placas 772633 marca Hyundai, Sedán de color gris ratón, el cual se encuentra a nombre de la coimputada Glenda Liseth Saenz, a Alejandro Papadopolo Moya y Glenda Liseth Sáenz, quienes, el primero de ellos acudió a varios comercios con las tarjetas falsas y pagaron con ella, obteniendo de este modo jugosas ganancias millonarias para todo el grupo delictivo., afectando con ello a los verdaderos titulares de las tarjetas, ya que las compras hechas por los acusados le generaron cargos, mientras que la segunda se presentó a diferentes cajeros automáticos realizando numerosos retiros de dinero. 2) Fue así como, durante el lapso de tiempo indicado anteriormente los imputados Papadopolo Moya y Sáenz Méndez, con la colaboración esencial entraron en posesión de tarjetas falsificadas las cuales fueron utilizadas para realizar diversas compras y retiros a indicar. Con este accionar los imputados influyeron en el normal procesamiento de los datos del sistema de cómputo del emisor de la tarjeta, mediante el uso indebido de datos de tarjetas obtenidos de un modo no especificado, perjudicando así al verdadero titular de la tarjeta y en última instancia al emisor. Tarjeta N°43809804-4846554. 3) Que el 29 de enero del 2013, en horas de la mañana, el imputado Donald Ureña Hernández abordó el vehículo 772633 desde la Ciudadela el Triunfo, Piedades de Santa Ana y recogió en Hatillo al señor Roberto Ortíz Finalet conocido como "Cubano", de inmediato se dirigieron hacía el sector de
Tibás, donde se reunieron con el co-imputado Alejandro Papadopolo Moya, luego se trasladaron al Centro Comercial IESA en Barrio México, lugar donde el imputado Alejandro Papadopolo Moya, ingresó al Centro Comercial, entre tanto los otros imputados esperaría por las cercanías en vía pública. 4) Fue así como, en ese lugar y al ser aproximadamente las 14:58 horas, el imputado Alejandro Papadopolo Moya se presentó al local Comercial IESA, y utilizó una copia o clon de la Tarjeta N° 4380 9804-484 6554, propiedad de la ofendida Ana Patricia Alfaro Camacho, e intentó realizar varias compras, siendo que le hizo creer a la dependiente Karen Miranda Villegas, que él era el verdadero dueño de la tarjeta, por lo que ejecutó la transacción por la suma a cancelar ¢690,162,32 colones, no obstante, la transacción salió denegada, por lo que el imputado le indicó que la volviera a pasar sólo por la mitad del precio y él cancelaría en efectivo el restante, por lo que la dependiente ejecutó un nuevo intento al ser las 14:59 horas esta vez por la suma de ¢345,081.00 colones y volvió a salir denegada. Ante esta situación el imputado le indicó que le guardara la factura que iría por efectivo, sin embargo, no volvió. De este modo, el acusado intentó obtener un beneficio patrimonial antijurídico por la adquisición de bienes de ¢690,163.32 colones en una primera instancia y de 345.000,81 colones en una segunda ocasión. Tarjeta N°4380980387137107. 5) El 31 de enero del 2013, en horas de la tarde, en los alrededores del Mercado Central de San José, como punto de reunión el imputado Donald Ureña Hernández y Roberto Ortiz Finalet, se re Cesar Francisco González Páez, dándose posteriormente un intercambio de manos de de un objeto indeterminado Ortiz Finalet y González Páez. Siendo que por avenida 4, se les acerco el co imputado Alejandro Papadopolo Moya, luego este se desplazó hasta el Centro Comercial Merayo y posteriormente a la Tienda Cavallini, lugar donde el imputado Alejandro Papadopolo Moya se bajó del vehículo conducido por Donald Ureña Hernández, entre tanto los otros co imputados esperaban en vía pública. 6) Fue así como, ese mismo día y en ese lugar, al ser aproximadamente las 15:22 horas, el imputado Alejandro Papadopolo Moya, se presentó al local Pastelería Merayo, y utilizó una copia o clon de la Tarjeta N° 4380 9803 8713 7107, perteneciente a Zhen Qiting, y realizó una compra, incidiendo con ello el sistema informático del ente emisor de la tarjeta, ya que le

hizo creer a la persona dependiente, que él era el verdadero dueño de la tarjeta, por lo que ejecutó la transacción por la suma a cancelar 2.500.00 colones, logrando con esto un beneficio patrimonial antijurídico para sí y para el grupo criminal con quien había ideado el plan por la suma de ¢2,500.00 colones, además para esa compra. 7) Con la utilización de esta tarjeta el imputado ALEJANDRO PAPADOPOLO MOYA, se trasladó hasta la Tienda Cavallini, sobre avenida I, San José, e ingresó a la tienda Relojería Cavallini, intentó realizar una compra por la suma de 209,950.00 colones, para cancelar mediante la utilización de la tarjeta Tarjeta N° 4380 9803 8713 7107, falsificada a su nombre a la persona dependiente, siendo que le hizo creer que él era el verdadero dueño de la tarjeta, por lo que ejecutó una transacción a las 15:37 horas por la suma de 209,950.00 colones, sin embargo, la transacción salió denegada, por lo que el imputado le indicó que volviera a pasar la tarjeta, acción que se realizó en dos ocasiones más, saliendo denegada. Ante esta situación el imputado se retiró del lugar. Tarjeta 41527611 58929120. 8) El 08 de enero del 2013, en el Cajero Autómatico de Citibank, ubicado en Santa Ana, haciendo uso de la tarjeta falsa, la acusada Glenda Lisseth Saénz, con la "tarjeta medio" es decir la tarjeta clonada y falsa número 4152-7611-5892-9120 que contenía la información bancaria del tarjetahabiente Isidro Reyes Romero, realizó los siguientes retiros 09:38:30 hrs la suma de ¢100.000.00 colones, a las 09:39:20 hrs la suma de ¢100,000.00 colones, al ser las 09:40:06 hrs la suma de ¢100,000.00 colones, con este accionar la imputada Glenda Liseth Sáenz en conturbenio con el imputado Donald Urefia Hernández, quien la transportó hasta el sitio y le proporcionó la tarjeta, influyeron en el normal procesamiento de los datos del sistema de cómputo, mediante la programación y empleo de datos falsos, así como el uso indebido de estos, perjudicando así al verdadero titular de la tarjeta y al ente emisor. 9) Nuevamente, el día 09 de enero del 2013 en el mismo lugar cajero de Citibank, Santa Ana, haciendo uso de esa misma Tarjeta indicada, la imputada Glenda Liseth Sáenz, realizó cuatro retiros consecutivos de dinero con la tarjeta falsa 4152 7611 5892 9120, propiamente a las 11:41:06 horas y 11 :41 :32 horas, dos retiros cada uno por la suma de ¢100,00.00 colones y dos retiros más a las 11:41:58 y 11:42:23 horas por la suma de ¢150.000 colones, y en el Lobby ATM 173 y 31 del Bac Fresh Market, Santa Ana realizó otros dos retiros por la suma de 200.000.00 colones colones cada uno, a las 11:40:47 y 11 :41:42 horas, de esta forma influyó el procesamiento de datos del emisor de la tarjeta y se impuso ella y los otros co imputados de un beneficio económico antijurídico. 10) Que la acusada Glenda Sáenz Méndez y los acusados Roberto Ortiz Finalet, Alejandro Papadopolo Moya y César González Páez no cuentan con antecedentes penales, mientras que Donald Ureña Hernández tiene un antecedente penal registrado" (sic; cfr. folios 545 a 550; el resaltado no es del original). Se declara sin lugar el motivo de casación. En el caso concreto la representación del Ministerio Público centra su disconformidad en la determinación de la relación concursal existente entre los hechos tenidos por acreditados y que fueron recalificados por el ad quem en la sentencia recurrida; específicamente: A) En relación con el imputado Alejandro Papadopolo Moya se revocó la calificación jurídica dada en la sentencia de instancia a los hechos sucedidos el 29 de enero del 2013 en el establecimiento comercial IESA y se dispuso recalificarlos como dos delitos de estafa informática en concurso ideal puesto que a criterio del ad quem “lo procedente es concluir que ambos delitos consumados, se ejecutaron mediante una única acción y por ende se trata de un concurso ideal de delitos y no uno material, consecuentemente […] debe sancionarse la acción ilícita mediante la aplicación del principio de aspiración, propio del concurso ideal, que faculta, más no obliga al juzgador, el aumento sobre la imposición más gravosa” (sic; folio 761 frente); se ordenó el reenvío para fijación de pena; B) En relación a la imputada Glenda Lisseth Sáenz Méndez, los jueces de apelación de sentencia también recalificaron los hechos tenidos por demostrados al considerarse que se trata de “un delito de estafa informática cometido el 8 de enero del 2013 y un delito de estafa informática cometido el 9 de enero del 2013, concurrentes materialmente y cuya penalidad ha de fijarse en juicio de reenvió (que este acto se ordena) conforme las reglas del delito continuado, respetando el principio de no reforma en perjuicio” (sic; folio 771 vuelto). Lo resuelto por el Ad Quem, en cuanto a ambas recalificaciones tiene efecto extensivo al imputado Donald Ureña Hernández por haber sido éste declarado coautor de los delitos de estafa informática antes referidos, ordenándose también para él el reenvió a juicio para la fijación de la pena. Así las cosas, no hay discusión en torno a la calificación de esos hechos como constitutivos del delito de estafa informática, debiendo entonces determinarse únicamente en esta sede, si tal y como lo afirma el Ministerio Público, el ad quem en la sentencia recurrida inobservó el artículo 76 del Código Penal y aplicó erróneamente el numeral 75 del mismo cuerpo normativo. Después del análisis de los argumentos planteados por la representación del Ministerio Público en el recurso de casación que se conoce, así como de la sentencia recurrida, se concluye que no existe el vicio alegado y que resulta ser conforme a derecho la recalificación que se hizo de los hechos acaecidos el 08 y 09 de enero del 2013 para el caso de la imputada Glenda Saénz Méndez, y en relación al imputado Alejandro Papadopolo Moya se identifica una fundamentación adecuada para proceder con la recalificación de los hechos por él cometidos el 29 de enero del 2013, debiéndose eso sí en esta sede de oficio, rectificar que en

atención al cuadro fáctico tenido por acreditado se está ante un único delito de estafa informática y no ante un concurso ideal de delitos, tal y como lo concluyó el ad quem , lo que resulta ser beneficioso para el imputado, y así se recalifica a efectos de su conocimiento en el juicio de reenvío para la fundamentación de la pena. El análisis sobre la unidad y pluralidad de acciones debe realizarse en cada caso concreto, y para ello se debe partir de tener claridad en torno a que las normas jurídico penales regulan conductas humanas que devienen en punibles y que dependen de la voluntad y finalidad de quien las ejecuta, de ahí que la unidad de acción debe entenderse como un concepto jurídico que no siempre resulta ser equivalente a la cantidad de acciones o movimientos corporales que se produzcan, de ahí que puede existir unidad de acción en un sentido jurídico y que ésta se encuentre compuesta a su vez de varios movimientos corporales o naturales, es por esa razón, que esta Cámara de Casación Penal, ha sostenido en reiteradas ocasiones que los elementos a tomarse en consideración para fijar el concepto de unidad de acción, están referidos no a la cantidad de acciones naturalmente ejecutadas por el agente, sino, a la estructura del tipo penal (factor normativo), así como su voluntad final (factor final), la cercanía o conexión temporal-espacial de los hechos, el bien jurídico tutelado y la unidad del sujeto pasivo. A efectos de establecer si nos encontramos ante una multiplicidad de delitos o bien, ante una unidad de acción, ha establecido esta Sala: “Al respecto hay que señalar que el concepto de acción no se refiere a acciones en sentido natural o físico, sino en sentido jurídico, para cuya determinación debe examinarse entre otras cosas, el fin perseguido por el sujeto activo, el hecho materialmente realizado, las condiciones de tiempo y lugar, así como las previsiones normativas acerca de la acción prohibida. Se ha establecido doctrinariamente lo siguiente: “…hay que excluir la identificación entre acción y movimiento corporal y la identificación entre acción y resultado. Una sola acción, en sentido jurídico, puede contener varios movimientos corporales (por ejemplo, violación intimidatoria, robo con fractura) o dar ocasión a que se produzcan varios resultados (hacer explosionar una bomba causando la muerte de varias personas). Son, pues, otros los factores que contribuyen a fijar el concepto de unidad de acción. El primero de ellos es el factor final, es decir, la voluntad que rige y da sentido a una pluralidad de actos físicos aislados (en el asesinato, la voluntad de matar unifica y da sentido a una serie de actos, como comprar y cargar la pistola, acechar a la víctima, apuntar o disparar; o, en el hurto, la voluntad de apropiarse de la cosa unifica y da sentido a los distintos actos de registrar los bolsillos de un abrigo. El segundo factor es el normativo, es decir, la estructura del tipo delictivo en cada caso en particular. Así, aunque el factor final que rige un proceso causal sea el mismo (matar a alguien), alguno de los actos particulares realizados puede tener, aisladamente, relevancia para distintos tipos delictivos (así, por ejemplo, la tenencia ilícita de armas de fuego para el delito de tenencia ilícita de armas). Y, a la inversa, actos aislados, cada uno regido por un factor final distinto, pueden tener relevancia típica solo cuando se dan conjuntamente (la falsificación de documentos privados solo es típica si se realiza con ánimo de perjudicar o perjudicando a un tercero) o tener una relevancia típica distinta (por ejemplo, robo con homicidio» (MUÑOZ CONDE, Francisco: Teoría general del delito, Valencia, Tirant lo blanch, 1991, pág. 194).” (Resolución 201100639, de las 15:40 horas del 27 de mayo de 2011, suscrita por las Magistradas Doris Arias, Jeannette Castillo, Lilliana García, María Elena Gómez y el Magistrado Rafael Sanabria. En similar sentido ver resoluciones 2019-01469, de las 11:45 horas del 15 de noviembre del 2019; 2019-00053, de las 11:57 horas del 18 de enero de 2019; 2018-460, de las 11:50 horas del 20 de junio de 2018)” . Precisamente el análisis de los indicados factores, permitió a los jueces del Tribunal de Apelación de Sentencia del II Circuito Judicial de San José, en la resolución recurrida, recalificar los hechos cometidos por Alejandro Papadopolo Moya el 29 de enero del 2013, y por Glenda Sáenz Méndez los días 8 y 9 de enero del 2013, puesto que contrario a lo establecido por el a quo en la sentencia de instancia, no se verifican en el caso concreto y en relación a lo acontecido en cada uno de esos días, acciones independientes que concurran materialmente entre sí, sino que por el contrario se está ante una única acción delictiva en los tres supuestos bajo análisis. Para arribar a esta conclusión, se debe partir de la configuración misma del tipo penal de estafa informática que está regulado en el artículo 217 bis del Código Penal: “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”. En la estafa informática el bien jurídico tutelado es el patrimonio, razón por la que la actividad fraudulenta del agente se relaciona con la manipulación del sistema informático para obtener un beneficio patrimonial antijurídico, de ahí que la utilización del cajero automático dándole órdenes para que dispensara tractos de dinero específicos y la tarjeta de crédito copiada que se utilizó para intentar pagar por bienes mediante transacciones que resultaron

denegadas, son el medio empleado por los imputados para alcanzar su finalidad delictiva de lesionar el patrimonio ajeno. Por otro lado, la estructura del tipo penal, hace alusión precisamente a la utilización de datos falsos para incidir en el procesamiento de los mismos por parte del sistema y lograr así el beneficio patrimonial indebido, y esto es precisamente lo que hacen los encartados. En el caso de Sáenz Méndez, queda claro de la lectura del cuadro fáctico acusado y tenido por demostrado, que la encartada realizó en cada uno de esos días, 08 y 09 de enero del 2013 respectivamente, una serie de acciones materiales que versaron en la utilización de la misma tarjeta falsa, sea la 4152 7611 5892 9120, con la que logró influir en el procesamiento de datos del mismo sistema informático del cajero automático del emisor de la tarjeta al que le dio órdenes de dispensa de dinero consecutivas que se producen como parte de un solo acto y persiguiendo la misma finalidad, ejecutadas de forma cercana en el tiempo y en el mismo espacio, de manera inmediata (con aproximadamente un minuto de diferencia entre una y otra), con identidad de sujeto pasivo y sujeto activo, por lo que constituyen una única acción en sentido jurídico penal, ya que denotan una sola resolución criminal, que no está interrumpida por factor alguno que evidenciara el cese en sentido estricto de la acción típica. La descripción fáctica de los hechos probados en torno a lo sucedido los días 8 y 9 de enero del 2013, no permite acreditar entonces, la existencia de acciones independientes que agoten cada una de ellas el tipo penal de la estafa informática, como lo pretende la recurrente. Así las cosas, en el presente caso, a partir de los hechos que se tuvieron por acreditados en sentencia de primera instancia, se determina que las conclusiones a las que arribó el ad quem son correctas y por ende, las acciones descritas como cometidas por la imputada Sáenz Méndez se deben tener como constitutivas de un delito de estafa informática cometido el 8 de enero del 2013 y un delito de estafa informática cometido el 9 de enero del 2013. Es importante, dejar en claro en este punto que a criterio del ad quem en el fallo recurrido, las acciones desplegadas por Sáenz Méndez los días 08 y 09 de enero del 2013, concursan entre sí materialmente, lo que no fue objeto de impugnación y no se entra a valorar en esta sede porque precisamente se dispone que en el juicio de reenvío deben aplicarse las reglas del delito continuado, respetando el principio de no reforma en perjuicio, de manera tal que este aspecto en particular no tiene incidencia en la pena a imponer en el caso concreto puesto que habiéndose determinado que entre lo sucedido en ambos días no hay una unidad de acción se descarta el concurso ideal y por ende, resulta ser más beneficioso para la encartada el que se apliquen las reglas de fijación de pena de conformidad con lo establecido en el artículo 77 del Código Penal, que las correspondientes al concurso material de delitos, según se establece en el numeral 76 del mismo cuerpo normativo. Ahora bien, en cuanto al imputado Alejandro Papadopolo Moya y en relación con los hechos por él cometidos el 29 de enero del 2013 en el local comercial IESA según la descripción fáctica tenida por acreditada y los razonamientos aquí esbozados, se desprende que la conducta delictiva realizada se ajusta también a un único delito de estafa informática y no a un concurso ideal delitos como equivocadamente lo concluyó el ad quem en la sentencia recurrida, puesto que se estableció que “el acusado intentó obtener un beneficio patrimonial antijurídico por la adquisición de bienes de ¢690,163.32 colones en una primera instancia y de ¢345.000,81 colones en una segunda ocasión”. Doctrinariamente se ha establecido que "...no es la unidad natural de acción la que dice cuando hay una acción en sentido legal; puede ocurrir, más bien, que una acción en sentido natural constituya legalmente una pluralidad de acciones o que una pluralidad de acciones en sentido natural constituya legalmente una sola acción. La separación entre unidad de acción y pluralidad de acciones solamente es posible mediante una interpretación del sentido del tipo penal realizado (CASTILLO: El Concurso..., págs. 19 a 20). La adopción del factor final (plan unitario que de sentido a una pluralidad de movimientos voluntarios como una sola conducta) y del factor normativo (que convierta la conducta en una unidad de desvalor a los efectos de la prohibición) como criterios para dilucidar cuándo hay una y cuándo varias conductas (ya se trate de acciones u omisiones) es ampliamente aceptada por la doctrina actual (así, ZAFFARONI, Op. cit., págs. 619 a 620; VELÁSQUEZ, Op. cit., págs. 584 a 588; MIR PUIG, Santiago: Derecho Penal Parte General, Barcelona, Promociones y Publicaciones Universitarias S.A., 1990, págs. 720 a 724; BACIGALUPO, Enrique: Principios..., pág. 280) y, en la medida que racionaliza fundadamente la aplicación de la ley sustantiva a partir del axioma de que la esencia del delito es la lesión a un bien jurídico tutelado, es adoptada por los suscritos…” (Sala Tercera de la Corte Suprema de Justicia. Sentencia Nº 943-98 de las 16:16 horas del 29 de setiembre de 1998). En el presente caso y partiendo de la descripción fáctica de los hechos tenidos por acreditados, se verifica que Papadopolo Moya actuó con un plan unitario en la realización de los hechos, determinándose con claridad el factor final de lograr el beneficio patrimonial indebido y esto mediante la utilización de la tarjeta clonada propiedad de Ana Patricia Alfaro Camacho, misma que entregó a la dependiente del local comercial IESA haciéndose pasar por el verdadero dueño de ésta y a efectos de pagar la misma factura por dos montos diferentes de dinero, siendo que a las 14:58 solicita que se pague la cuenta y al resultar rechazada la gestión, de manera inmediata pide a la dependiente del local comercial que lo intente de

nuevo por un monto menor al primero sin lograr tampoco en esta oportunidad que se haga efectivo el pago, de ahí que se retira del lugar, de manera tal que el factor normativo hace que esas conductas sean una unidad de desvalor a los efectos de la prohibición, cumpliéndose con ello el factor normativo del tipo penal de Estafa Informática, es decir que realizó dos transacciones separadas por un tiempo aproximado de un minuto lo que no rompe la conexión espacio temporal entre ellas, que recayeron sobre el mismo objeto material que es el mismo sistema informático y afectando el mismo bien jurídico puesto que se puso en peligro el patrimonio del mismo sujeto pasivo, sea la verdadera titular de la tarjeta, haciéndose necesario acudir al concepto de unidad de acción en sentido jurídico, puesto que con una única acción se lesiona la misma disposición legal, sea la estafa informática, cuyo bien jurídico es el patrimonio. En resumen, a criterio de esta Cámara de Casación Penal, entre los diferentes actos materiales ejecutados en el mismo día, lugar y con la utilización de la misma tarjeta, por los imputados Papadopolo Moya (hechos del 29 de enero del 2013 en donde se da un primer intento de pago a las 14:58 horas y uno posterior inmediato a las 14:59 horas, ambos con la misma tarjeta y en el mismo establecimiento IESA,), y Sáenz Méndez (A) Hechos del 08 de enero del 2013: tres retiros con la misma tarjeta en el cajero automático de Citi Bank Santa Ana, realizados a las 09:38:30 hrs, 09:39:20 hrs y 09:40:06 hrs; y B) Hechos del 09 de enero del 2013: dos retiros con la misma tarjeta en el cajero automático de Fresh Market Santa Ana, realizados a las 11:40:47 hrs y a las 11:41:42 hrs), existe unidad de acción que responde a una sola intencionalidad inmediata y específica, son acciones conexas por la finalidad de afectar el patrimonio de la misma persona ofendida y se caracterizan por la cercanía espacio temporal de ocurrencia, por lo que se descarta la existencia de delitos independientes que concurren materialmente entre sí, de ahí que no lleva razón en sus alegatos recursivos el Ministerio Público. En atención a todo lo expuesto y de conformidad con los hechos tenidos por demostrados en el caso concreto, el conocimiento y la voluntad de Papadopolo Moya y de Sáenz Méndez, no era cometer varios delitos en un mismo momento y lugar, puesto que incluso en cada evento el ofendido era la misma persona titular de las cuentas respectivas por lo que el sujeto pasivo es el mismo, como también lo es el bien jurídico tutelado que resulta lesionado lo que implica una sola acción en sentido jurídico penal y evidencian una sola resolución criminal. Se concluye entonces, que la conducta típica desplegada por los imputados en cada uno de los días mencionados en los hechos probados de la sentencia de primera instancia (08, 09 y 29 de enero del 2013) se exteriorizó mediante una pluralidad de acciones ejecutadas de forma cercana en el tiempo y espacio, de manera inmediata o sucesiva, con identidad de sujeto pasivo y activo, con una única finalidad no interrumpida por factor alguno, de ahí que la recalificación que determinó el ad quem en el fallo recurrido, en cuanto a la imputada Glenda Lisseth Saénz, está conforme a derecho y se adecua al cuadro fáctico demostrado, por lo que no existe una errónea aplicación de la ley sustantiva, y se mantiene incólume lo resuelto. En relación con el imputado Alejandro Papadopolo Moya, se recalifican los hechos cometidos el 29 de enero del 2013 a un delito de estafa informática. En apego a lo establecido en el artículo 443 del Código Procesal Penal, lo resuelto tiene efecto extensivo para con el imputado Donald Ureña Hernández por haber sido éste declarado coautor de los delitos de estafa informática cometidos con Alejandro Papadopolo Moya el 29 de enero del 2013 y con Glenda Sáenz Méndez el 8 y 9 de enero del 2013.

Por Tanto:

Se declara sin lugar el recurso de casación interpuesto por la representante fiscal, licenciada Ruth María Quesada

Quesada. Consecuentemente, se mantiene incólume lo resuelto por el Tribunal de Apelación de Sentencia Penal del Segundo Circuito Judicial de San José, Goicoechea, en cuanto a la recalificación de los hechos ejecutados por la imputada G.L.S. De oficio, se recalifican los hechos cometidos por el imputado A.P.M. el 29 de enero del 2013, a un delito de estafa informática y se mantiene el reenvío para la fundamentación de la pena correspondiente. De conformidad con lo establecido en el artículo 443 del Código Procesal Penal, lo resuelto tiene efecto extensivo al imputado D.U.H. por haber sido éste declarado coautor de los delitos de estafa informática antes mencionados. Se mantiene lo dispuesto en torno a la orden de reenvió de la causa para la determinación de la

pena correspondiente a los tres imputados, debiéndose respetar el principio de no reforma en perjuicio. Notifíquese.

Patricia Solano

Álvaro Burgos

Gerardo Rubén Alfaro

Sandra Eugenia Zúñiga

Ronald Cortés
Magistrado

RVILLEGA
1261-3/7-1-