UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

FACULTAD DE DERECHO

TRABAJO FINAL DE GRADUACION PARA OPTAR POR EL GRADO DE MAESTRIA EN DERECHO PENAL

TITULO

RETOS DE LA INDIVIDUALIZACIÓN DE LA PERSONA AUTORA DEL DELITO DE ESTAFA INFORMÁTICA

ESTUDIANTE

JHONNY ANTONIO ROJAS DIAZ

TUTORA

ODILIE ROBLES ESCOBAR

SEDE CENTRAL

MAYO 2024

Tabla de contenido

Capítulo I: Problema

Planteamiento del problema

El problema del tema de la investigación considera que, debido a la naturaleza virtual del delito, es difícil identificar a las personas responsables del hecho ilícito. Esto se debe a que los delitos informáticos suelen cometerse desde lugares remotos, utilizando herramientas que dificultan el rastreo de los delincuentes.

En Costa Rica, el delito de estafa informática está tipificado en el artículo 217 bis del Código Penal, que establece que:

> Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.
>
> La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Por lo que establece la ley, para que se configure el delito de estafa informática, es necesario que se cumplan los siguientes elementos:

1. Que haya una persona que resulte defraudada.
2. Que haya un engaño o artificio utilizado para cometer la estafa.
3. Que la estafa se cometa mediante el uso de una computadora u otro medio electrónico, informático o telemático.
4. Que haya un beneficio económico o una disminución de una obligación patrimonial para el estafador, (Castro, 1987, pp. 81-82).

La dificultad para individualizar al autor o autores del delito de estafa informática en Costa Rica se debe a los siguientes factores:

1. El anonimato: Los delitos informáticos suelen cometerse desde lugares remotos, utilizando herramientas que dificultan el rastreo de los delincuentes.
2. Se presenta la dificultad para obtener pruebas: Las pruebas de los delitos informáticos suelen ser digitales, lo que dificulta su obtención y análisis.
3. La complejidad de las técnicas utilizadas: Los delincuentes informáticos suelen utilizar técnicas sofisticadas que dificultan su identificación.
4. Los retos que plantea la individualización del autor o autores del delito de estafa informática en Costa Rica han llevado al desarrollo de nuevas técnicas de investigación, estas técnicas incluyen el uso de análisis de redes sociales, análisis de tráfico de internet y análisis de malware. (Castro, 1987, p. 85).

A pesar de estos avances, la individualización del autor o autores del delito de estafa informática sigue siendo un reto importante en Costa Rica, por las siguientes razones:

1. La naturaleza virtual del delito: El delito de estafa informática se comete en el espacio virtual, lo que dificulta la identificación de los autores. Los delincuentes suelen utilizar métodos para ocultar su identidad, como el uso de proxies, VPNs y otros softwares de enmascaramiento.
2. La complejidad de las técnicas utilizadas: Los delincuentes utilizan técnicas cada vez más sofisticadas para cometer estafas informáticas. Esto dificulta que las autoridades policiales puedan rastrearlos y detenerlos.
3. A las anteriores dificultades se une la falta de recursos: Las autoridades policiales costarricenses cuentan con recursos limitados para investigar los delitos informáticos. Esto dificulta que puedan seguir el rastro de los delincuentes y recopilar pruebas suficientes para su identificación. (Bonilla, 2019, pp. 223-224).

Conviene describir con más detalle algunas de estas dificultades:

La naturaleza virtual del delito, la estafa informática se comete a través de Internet, lo que dificulta la identificación del lugar de comisión del delito. Esto puede dificultar la cooperación entre las autoridades policiales de diferentes países.

La complejidad de las técnicas utilizadas, los delincuentes utilizan técnicas como el phishing, el malware y el ransomware para engañar a las víctimas y robarles sus datos personales o financieros. Estas técnicas pueden ser difíciles de detectar y rastrear.

La falta de recursos del Estado, como se ha señalado anteriormente, las autoridades policiales costarricenses cuentan con un número limitado de agentes especializados en delitos informáticos. Además, la tecnología utilizada por las autoridades policiales puede ser inferior a la utilizada por los delincuentes.

Para superar estas dificultades, las autoridades de la policía judicial han adoptado una serie de medidas, como lo son la cooperación internacional, para ello trabajan en estrecha colaboración con las autoridades policiales de otros países para investigar los delitos informáticos. Se ha hecho necesario que se brinde una constante capacitación de los agentes policiales en cuanto a técnicas de investigación de delitos informáticos.

Por lo anotado anteriormente, se justifica la inversión en tecnología para mejorar su capacidad de investigar los delitos informáticos. Sin embargo, estas medidas aún no han sido suficientes para resolver el problema de la impunidad en los delitos informáticos en Costa Rica.

El problema de investigación identifica un aspecto concreto que es la dificultad de identificar a los autores de delitos de estafa informática en Costa Rica, siendo el definido para el presente trabajo el siguiente:

¿Cuáles son los retos que plantea la individualización de la persona autora del delito de estafa?

A continuación, con el fin de sistematizar el problema se presentan una serie de interrogantes que tienen una relación directa con el objeto de estudio:

1. ¿Cómo puede mejorarse la eficacia de la investigación y el procesamiento de los casos de estafa informática en Costa Rica?
2. ¿Qué papel pueden jugar las nuevas tecnologías en la lucha contra la estafa informática?
3. ¿En qué medida el anonimato dificulta la individualización del autor o autores del delito de estafa informática?
4. ¿Cuáles son las dificultades para obtener pruebas en los casos de estafa informática?

5. ¿Cómo se pueden contrarrestar las técnicas sofisticadas utilizadas por los delincuentes informáticos?

Estas sub-preguntas pueden ayudar a identificar los aspectos clave del problema y su objetivo es guiar la investigación y el análisis sobre este tema.

Objetivos

Objetivo general

Analizar los retos que plantea la individualización del autor o autores del delito de estafa informática en Costa Rica del periodo 2018 a 2023.

Objetivos específicos

1. Indagar los factores que contribuyen a la dificultad para individualizar al autor o autores de los delitos de estafa informática en base a la entrevista a profundidad realizada a los informantes claves.

2. Identificar las técnicas de investigación que actualmente se utilizan a través de la entrevista a profundidad a expertos del Poder Judicial que estén a cargo de la investigación del delito de estafa informática.

3. Determinar a través de la jurisprudencia costarricense sobre los casos de estafa informática para identificar las dificultades en la individualización del autor o autores de la esta informática.

Justificación

Este delito constituye un problema creciente en Costa Rica, según datos de la Policía Judicial, en 2022 se registraron más de 10.000 casos de estafa informática, un aumento del 20% con respecto al año anterior. (Bermúdez, 2019, p.4).

Este aumento es preocupante, ya que la estafa informática tiene un impacto negativo en la economía y en la sociedad. Las víctimas de este delito suelen sufrir pérdidas económicas significativas y también pueden sufrir daños psicológicos.

La dificultad para individualizar al autor o autores del delito de estafa informática dificulta la investigación y el procesamiento de estos casos. Esto hace que sea más difícil sancionar a los delincuentes y prevenir futuros delitos. Por lo tanto, es importante estudiar los retos de la individualización del autor o autores del delito de estafa informática, con el fin de desarrollar nuevas técnicas de investigación que permitan mejorar la eficacia de la lucha contra este delito.

Además, los siguientes argumentos específicos pueden justificar el tema de estudio:

1. El aumento de los casos de estafa informática: El número de casos de estafa informática ha aumentado significativamente en los últimos años, lo que indica que este delito es un problema creciente.
2. El impacto negativo de la estafa informática: La estafa informática tiene un impacto negativo en la economía y en la sociedad. Las víctimas de este delito suelen sufrir pérdidas económicas significativas, y también pueden sufrir daños de carácter psicológico.
3. La dificultad para individualizar al autor o autores del delito: La dificultad para individualizar al autor o autores del delito de estafa informática dificulta la investigación y el procesamiento de estos casos.

Estos argumentos demuestran que el tema "Los retos de la individualización de autor o autores del delito de la estafa informática" es un tema relevante y de actualidad que requiere ser estudiado con profundidad con el fin de buscar la mejor solución del mismo.

Antecedentes

Estos incluyen la definición del delito de estafa informática, sus elementos constitutivos y las penas que se aplican por su comisión, las técnicas y herramientas que se utilizan para investigar delitos informáticos y además se debe conocer la legislación costarricense que regula los delitos informáticos.

Estudios sobre la prevalencia de la estafa informática en Costa Rica, son importantes por cuanto pueden proporcionar información sobre la magnitud del problema de la estafa informática en Costa Rica. El estudio de Bermúdez (2019) de delitos informáticos en Costa Rica, se sextuplican en cinco años y desbordan a policía es pertinente por cuanto hace referencia a las declaraciones brindadas por el fiscal general y el jefe de la OIJ en torno al incremento de la delincuencia cibernética en Costa Rica, de las cuales se extraen estudios sobre las técnicas utilizadas por los delincuentes informáticos, los cuales pueden ayudar a comprender cómo los delincuentes informáticos cometen estafas informáticas.

La ciberdelincuencia es un fenómeno en constante evolución, por lo que es importante estar al día de las últimas técnicas utilizadas por los delincuentes informáticos. A continuación, se presentan algunos estudios que analizan estas técnicas: El estudio de "Técnicas utilizadas por delincuentes informáticos para realizar fraudes vía medios electrónicos", de Martha Isabel Orozco Donado (2011) interesa para la presente investigación por cuanto describe las técnicas más utilizadas por los ciberdelincuentes para apropiarse de información confidencial y a su vez obtener bienes y servicios de personas que utilizan medios electrónicos en el momento de realizar operaciones financieras.

El estudio realizado por Marc Bernaldo, Las 15 técnicas de hacking más comunes, de ESED interesa presenta una lista de las técnicas de hacking más utilizadas. “El estudio contribuye por cuanto expone los métodos que utilizan los ciberdelincuentes para vulnerar la seguridad de un sistema o infraestructura informática, normalmente con el fin de robar información o datos valiosos, poniendo a la empresa en un aprieto”, (Bernaldo, 2023, p.1). El objetivo del estudio es mantener la seguridad de un sistema. En el estudio se transcriben las 15 técnicas de hacking más comunes con el fin de considerarlos en la presente investigación.

El antecedente titulado "Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse", del Instituto Nacional de Ciberseguridad de España (2023), es de importancia para la presente investigación por cuanto explica cómo los ciberdelincuentes utilizan la ingeniería social para engañar a las víctimas y obtener su información confidencial. Para el presente estudio es importante porque ofrece las técnicas que utilizan los ciberdelincuentes en los ataques de ingeniería social a pesar de ser múltiples y varias las técnicas utilizadas por los ciberdelincuentes para manipular a sus víctimas suelen seguir una serie de principios básicos que se ofrecen en este estudio.

El impacto económico de la ciberdelincuencia en España del Centro Nacional de Ciberseguridad, es un informe que estima que el impacto económico de la ciberdelincuencia en España alcanzó los 10.000 millones de euros y el 2021 ha sido el año en el que más incidentes críticos se han gestionado desde el CCN-CERT. Es de importancia a esta investigación porque añade que en líneas generales los incidentes han demostrado una mayor sofisticación, especialmente a través de vulnerabilidades de ejecución remota de código (RCE, del inglés remote code execution) de tipo día cero, pero también mediante el compromiso de la cadena de suministro, tal y como apuntaba la tendencia en 2020. El estudio señala que el año de las vulnerabilidades, tal y como se pudo observar desde el primer trimestre de 2021, el término vulnerabilidad ha sido una constante a lo largo de ese año.

La tesis de Brandon Álvarez González y Alex Villegas Carranza. “Propuesta de un estándar nacional que facilite determinar la admisibilidad de la evidencia digital en delitos informáticos en Costa Rica”, (2022), es de importancia para el presente estudio por cuanto señala que mucha de la información recopilada durante el estudio sobre las prácticas utilizadas en Costa Rica para ejecutar una investigación en cómputo forense fue extraída de entrevistas a expertos y profesionales en el área. Esto se debe a que en Costa Rica la información pública sobre los procedimientos, técnicas o métodos a seguir en la investigación forense es escasa o inaccesible.

"El estado de la ciberseguridad en el mundo", de la empresa de seguridad Kaspersky (2023), es un informe que analiza las principales tendencias en ciberseguridad a nivel mundial. Contribuye al presente estudio por cuanto señala que, en Barcelona, en medio de uno de los eventos de tecnología más grandes del mundo, el Mobile World Congress (MWC), Marc Rivero, analista sénior de seguridad de Kaspersky, dijo a DPL News que es necesario trabajar en entornos digitales

seguros que contemplen las novedades de las nuevas tecnologías como las redes 5G, el Internet de las cosas (IoT) y la Inteligencia Artificial (IA). Por ello, Kaspersky presentó su ecosistema de ciberseguridad con el que pone a disposición de compañías de todo tamaño las soluciones que les permiten proteger la información y los datos sensibles sin rezagarse de la transformación digital.

La publicación que realiza el MICITT, (2023). Costa Rica Estrategia Nacional de Ciberseguridad 2023-2027, contribuye a este estudio porque ofrece una esta estrategia nacional que plantea que es de suma importancia para la realización de la presente investigación la cual plantea que en las últimas décadas se ha incrementado exponencialmente el uso de las Tecnologías de la Información y la Comunicación (TIC) y las oportunidades socioeconómicas y políticas que se derivan de ello (CEPAL, 2018). La transformación digital que se está viviendo a nivel global es un poderoso facilitador de un desarrollo inclusivo y sostenible, pero también puede presentar una nueva fuente de problemas si la infraestructura subyacente y los servicios que dependen de ella no son seguros ni están protegidos frente a las amenazas cibernéticas.

Carrera Peña, Iveett del Rosario, tesis de Maestría titulada Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima (2021). Universidad César Vallejo. Programa Académico de Maestría en Derecho Penal y Procesal. Es de interés para este estudio porque plantea como objetivo general, determinar las deficiencias en las investigaciones por delito de fraude informático en el distrito de Lima. Entre sus objetivos se buscó analizar cómo la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima. Como resultado se pudo determinar que las principales deficiencias es la falta de capacitación a las diversas modalidades informáticas que se presentan en la actualidad, perjudicando el curso y dirección de las investigaciones fiscales por estos ilícitos, la misma que además no cuenta con un respaldo normativo.

El estudio clave para identificar la ciberdelincuencia en las redes sociales, se considera como una importante fuente de información para la presente investigación, porque: el organismo Global Web Index (2022) realiza un reporte periódico en el cual informa cuántas horas diarias pasa una persona en las redes sociales según la región. En Latinoamérica, un usuario promedio interactúa con estas plataformas alrededor de 3 horas y 34 minutos por día, mientras que la cifra a nivel global es de 2 horas y 28 minutos. Se deduce que esa intensa conexión en estos espacios

virtuales genera vínculos sociales, comunicación entre individuos y hasta relaciones laborales y como consecuencia aumenta la exposición a amenazas relacionadas con la ciberdelincuencia.

Proyecciones

Las proyecciones del desarrollo del tema "Retos en la individualización de la persona autora del delito de estafa informática" son positivas. El aumento de la prevalencia de la estafa informática, la evolución de las técnicas utilizadas por los delincuentes informáticos y el impacto negativo de este delito, hacen que sea necesario desarrollar nuevas investigaciones sobre este tema.

1. Mejorar la comprensión de los retos que plantea la individualización del autor o autores del delito de estafa informática.
2. Evaluar la eficacia de las técnicas de investigación utilizadas actualmente.
3. Proponer soluciones efectivas para mejorar la eficacia de la investigación y el procesamiento de los casos de estafa informática.
4. Favorecer mejoras de la lucha contra la estafa informática en Costa Rica. El aumento de la eficacia de la investigación y el procesamiento de los casos de estafa informática podría ayudar a reducir la prevalencia de este delito y a proteger a las víctimas.

A continuación, se presentan algunas proyecciones específicas del desarrollo de este tema:

1. Promover el desarrollo de nuevas técnicas de investigación que permitan superar los retos actuales.
2. El fortalecimiento de las capacidades de los investigadores para investigar casos de estafa informática.
3. La implementación de políticas públicas para prevenir la estafa informática.

El desarrollo de este tema podría contribuir a la mejora de la lucha contra la estafa informática en Costa Rica. El aumento de la eficacia de la investigación y el procesamiento de los casos de estafa informática podría ayudar a reducir la prevalencia de este delito y a proteger a las víctimas.

Capitulo II: Marco Teórico

Conceptualización del delito de estafa informática

El engaño

El engaño ha sido utilizado en muchas manifestaciones por parte de los delincuentes para cometer sus delitos, este se puede entender como "la acción o el resultado de presentar lo que no es cierto como verdad, lo que aparenta ser verdad cuando es mentira, o el efecto de hacer creer mediante palabra u obra, lo que no es o lo que es diferente a lo real" (Diccionario Poder Judicial,2022).

El engaño significa: Falta de verdad en lo que se dice, hace, cree, piensa o discurre. Según el Diccionario de la Real Academia Española (RAE 2020) engaño posee las siguientes acepciones, de las cuales se transcriben las que interesan para el estudio:

1. Acción y efecto de engañar.
2. Falta de verdad en lo que se dice, hace, cree, piensa o discurre.
3. Satisfacer, desengañar, sacar del engaño y error aprehendido.
4. Retraerse de lo pactado, por haber reconocido engaño en el contrato, o pretender que se deshaga algo, alegando haber sido engañado.

En el caso de la estafa informática, cita Velasco (2019), "usando anonimizadores y malware, realizan ataques en el mundo cibernético con consecuencias semejantes a quien lo hace en el mundo físico, pero con la ventaja de que impiden y neutralizan una reacción física de la víctima que, cuando descubre el engaño, no puede replicar, al menos físicamente" (p. 25), el acceso a la tecnología significa una gran ventaja cuando se trata de conseguir una distancia física del delincuente con su víctima, como bien lo cita el autor, el engaño por medio de internet garantiza la protección de la integridad física del delincuente, esto visto desde la distancia, y sobre todo permite mantener segura su identidad y con ello la dificultad de poder ser acusado del delito.

> La sociología: que precisa del engaño a otro ser humano, mediante cualquier fórmula de ingeniería social, que con cierta entidad (engaño bastante, y no mera exageración o retruécano comercial, o simple dolus bonus) produce error en su víctima de manera que le

> induzca a realizar un acto de disposición con contenido económico no querido en perjuicio propio o de tercero, (Velasco, 2019, p. 28).

El autor describe como la sociología es una modalidad de como obtienen lucro los delincuentes, siendo el engaño la principal forma en los delitos informáticos, lo cual cuenta con un sentido lógico en la forma de idear el plan en la mente del delincuente, desde las primeras etapas del iter criminis el autor del delito busca el aprovechamiento del internet para la protección de su identidad, con lo cual, al no estar físicamente en la escena del crimen, es el engaño su medio para ejecutar su plan, al engañar a la víctima por medios tecnológicos, la víctima se representa en una escena segura para ella físicamente, donde no está siendo amedrantada para despojarla de su patrimonio, por lo que esa barrera física es segura en la representación de la víctima, por lo que cae en una falsa representación de que lo que está sucediendo es seguro y confía en lo que el delincuente quiere que realice.

Nuestra legislación penal tipifica el engaño por medios tecnológicos, el primer párrafo del artículo 217 bis del Código Penal dice:

> 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.

Es en las palabras “influya en el ingreso” donde se configura el engaño del delincuente a la víctima, se debe de comprender que para que se produzca una estafa informática esta depende de alguna medida de seguridad que sea vencida por el delincuente, pudiendo ser por el sistema informático con deficiente seguridad o acceso a través de la víctima.

Las victimas facilitan dicha información ante situaciones engañosas, como lo son la noticia de haber ganado un premio, revisar su tarjeta por ser utilizada, esto en caso de llamadas telefónicas, pero también puede suceder con paginas creadas por los hackers con una similitud idéntica a

paginas oficiales, en donde si la víctima no verifica la dirección IP puede brindar sus accesos y estos ser utilizados por los delincuentes.

De acuerdo con Castro (2018, pág.79)

> Todas las disciplinas jurídicas están afectadas por la informática y lo penal no es la excepción, todo lo contrario, podemos afirmar que es quizá la rama jurídica en la que la computación juega un papel muy interesante y particular. Partimos de que la computadora, como herramienta, constituye la generalidad de las veces el instrumento del que eventualmente se puede servir el delincuente, para realizar su acción ilegítima, pero sin embargo en cierta medida, con el propio avance de la informática se hará necesario regular con mayor precisión los tipos penales, de manera que las conductas queden más claramente delineadas.

Considerando que los delitos informáticos se han convertido en la actualidad en los hechos delictivos con mayor incidencia a nivel mundial, y particularmente a nivel nacional, las nuevas formas de delinquir han justificado la creación de leyes que penalicen dichos delitos informáticos para sancionar con fundamento legal a quienes incurran en los mismos. De esta manera, en el año 2001 se promulga la Ley 8148 que se adiciona al Código Penal de Costa Rica para incluir los artículos de Violación de Comunicaciones Electrónicas (196 bis), Estafa o Fraude Informático (217 bis) y Alteración de Datos y Sabotaje Informático (229 bis).

Interesa señalar lo que expresa Tiederman (1985) en su obra Poder Económico y Delito en (Castro 1987, pág. 82) en relación con este tipo de normativas:

> El tipo penal de la falsificación de documentos exige que el documento sea la expresión tangible y probatoria de un pensamiento humano. Aunque se cuestione este requisito, los datos archivados electrónicamente no son reconocibles visualmente. Por lo general, además, no permiten individualizar autores.

De la anterior cita se destaca uno de los objetivos de esta investigación que consiste en tomar como objeto de estudio el requerimiento de establecer una estrategia eficiente y eficaz para superar los retos de la individualización.

Según lo establece Laura Mayer Lux (2014, p. 2) en “El engaño concluyente en el delito de estafa” Revista chilena de derecho, versión On-line ISSN 0718-3437:

> El engaño "concluyente" en el delito de estafa ha sido reconocido fundamentalmente en materia de estafa de consumo, cuyo caso más pintoresco es el denominado "perro muerto", expresión empleada en algunos países latinoamericanos para aludir a quien se retira de un restaurante sin pagar la cuenta de lo que consumió.
>
> El concepto de "engaño concluyente" no se limita al tipo penal de estafa, pese a haber encontrado en él su máxima expresión. Es más, ni siquiera se circunscribe al Derecho Penal, pudiendo extenderse a toda relación comunicativa en la que sea posible construir una afirmación (falsa) mediante un proceso deductivo, afirmación que, por eso mismo, pasará a ser implícita e indirecta. Incluso más allá del concepto de engaño, el Derecho civil de los actos jurídicos reconoce ampliamente la posibilidad de emitir una declaración de voluntad a través de "actos concluyentes".

Por lo tanto, lo que diferencia al engaño concluyente en la estafa de otros engaños concluyentes, es tanto el criterio que ha de utilizarse para efectuar el proceso deductivo, como los hechos a los que debe referirse la afirmación falsa en cuestión. Tratándose de declaraciones concluyentes de voluntad, además del criterio para realizar la deducción y el objeto del mensaje de que se trate, variará el objeto del proceso deductivo mismo: mientras que en el engaño concluyente se deduce una afirmación (falsa) sobre hechos, en las declaraciones concluyentes de voluntad se deduce, precisamente, la voluntad de la parte que la emite (Mayer, 2014).

Según Ruiz Ezquerro (2019, p.11) el engaño ha de ser causante, bastante y antecedente, cabe recalcar el “bastante” dentro de estos tres ya que puede dar lugar a que una conducta que a priori pueda parecer engañosa, quizá no lo es con suficiente entidad como para inducir al error del sujeto pasivo.

Caracterización de la víctima, al conocer un poco las acciones de las que podemos ser víctimas surge la duda de quién es realmente se pueden ver afectados por estas acciones o delitos. Al respecto señala Orozco Donado (2011, p.5):

> Una víctima de fraudes de tipo electrónico será entonces una persona que tenga acceso a estos medios, en el caso de víctimas de delitos financieros serán sin duda las persona que tengan edad suficiente para ingresar al sistema financiero, es decir que puedan adquirir productos y hacer uso de ellos a través de medios electrónicos.

Así se saca como conclusión que de acuerdo con Orozco Donado (2011, p. 6) de sus estudios realizados en la Facultad Ingeniería de sistemas, Universidad Piloto de Colombia:

La víctima no se caracteriza por un nivel sociocultural específico debido a que estos delitos son inherentes al grupo social y afectan indistintamente a personas de diferentes estratos y niveles, por lo que es evidente la incursión del uso de Internet en todos los estratos en algunos a menos escala, pero esa situación está cambiando y va en incremento anual gracias al programa Vive Digital. (p. 6)

El perjuicio patrimonial

El concepto de perjuicio es muy amplio, en el sentido que puede ser utilizado para todas las ramas del derecho, en el caso de la estafa el perjuicio cobra una importante relevancia, puesto este se comprende como la afectación al bien jurídico protegido de la propiedad de la víctima, siendo una definición para el perjuicio la siguiente:

> En una terminología ampliamente difundida, el injusto propio del delito de estafa es el resultado de la relación entre el desvalor de la acción constituida por el engaño típico y el desvalor del resultado, constituido por la disposición patrimonial perjudicial. El perjuicio patrimonial como resultado de la acción desplegada por el agente es determinante a la hora de configurar el resultado del delito de estafa, que no puede diferenciarse del acto de disposición (Gutiérrez, 2013: 451). Es así que dicho perjuicio debe consistir en un detrimento patrimonial asociado directamente a la disposición de la víctima, que se traduce en una acción o una omisión. En los términos propios de la dogmática del delito de estafa, esto se presenta como una exigencia de inmediatez entre la disposición y el perjuicio (Mañalich, 2010: 344; Muñoz Conde, 2007: 426 y 430). (Caro, 2019, p. 114).

El perjuicio se relaciona propiamente con la afectación que recibe la víctima del acto del delincuente, siendo este indudablemente un daño que conlleva un perjuicio en su patrimonio, siendo el delito de estafa informática una modalidad de estafa, la cual pretende desprender de su patrimonio a la víctima, siendo en su mayoría dinero de su cuenta bancaria.

Ante una estafa informática, siempre procura el delincuente el engañar a su víctima de forma anónima, valiéndose de la barrera tecnológica que esta le proporciona una distancia segura

para actuar en el anonimato, el delito lo configura ese menoscabo patrimonial que no se hubiera producido por el hecho dañoso del delincuente.

Se deduce que el perjuicio patrimonial es un elemento esencial de los delitos informáticos en Costa Rica. Este perjuicio puede consistir en la pérdida o disminución del patrimonio de la víctima, o en el lucro obtenido por el delincuente.

Por lo tanto, para que se configure el perjuicio patrimonial, es necesario que sea real y que sea consecuencia directa del delito informático. El perjuicio debe ser cuantificable, es decir, debe determinar su valor económico.

Se hace constar de la normativa vigente como ejemplos de perjuicios patrimoniales que pueden ser causados por delitos informáticos:

1. Robo de información confidencial. El robo de información confidencial, como datos financieros o datos personales, puede causar un perjuicio económico a la víctima si esta información es utilizada para cometer fraudes o extorsiones. (Código penal, aartículo 196 bis. - Violación de datos personales)

2. Denegación de servicio. Un ataque de denegación de servicio puede causar un perjuicio económico a la víctima si la interrupción del servicio le ocasiona pérdidas de ventas o de productividad, (Código penal, aartículo 229 ter. - Sabotaje informático)

3. Virus informáticos. Un virus informático puede causar un perjuicio económico a la víctima si destruye o corrompe sus datos. (Código penal Artículo 229.- Daño agravado)

El perjuicio patrimonial es un elemento importante para la persecución de los delitos informáticos. Este elemento permite que las autoridades judiciales puedan castigar a los delincuentes y que las víctimas puedan obtener reparación por el daño sufrido.

El perjuicio patrimonial en el delito de estafa informática es un elemento esencial para la configuración del tipo penal. Se trata de la disminución o pérdida del patrimonio del sujeto pasivo, causada por la actuación del sujeto activo.

El ánimo de lucro

El ánimo de lucro se define como “Intención o propósito de obtener o poseer una ganancia, utilidad o provecho, generalmente económico” (Diccionario Poder Judicial, 2020), este concepto no debe de entenderse como un delito, por el contrario, el ánimo de lucrar es un cuando una persona decide aumentar su patrimonio, por lo general de forma licita, sin embargo, también se puede aumentar el capital de manera ilícita, por lo que es este aumento de capital la motivación a cometer los delitos, siendo la estafa un delito que busca el aumento del patrimonio, esto con el despojo del dinero de sus víctimas.

El ánimo de lucro en el ciberdelito en Costa Rica se castiga aumentando la pena prevista para el delito en cuestión, el artículo 217 bis del código penal establece dos clases de pena, de tres a seis años cuando el delito es perjuicio de persona física o jurídica, o de cinco a diez años en perjuicio de sistemas de información pública, bancarios, estas penas aumentan en sus extremos mínimos si los comparamos con el delito de estafa del artículo 216 del código penal.

El ánimo de lucro es una característica propia de los delitos que pretenden un aumento de patrimonio del autor del delito, el cual debe ubicarse en el tipo penal como un elemento subjetivo, donde el autor comete el acto dolosamente, con la única intención de despojar de su patrimonio a la víctima y lucrar para sí o un tercero, este aprovechamiento del bien jurídico ajeno es cometido con sistemas informáticos elaborados para engañar a sus víctimas.

El ánimo de lucro se presume cuando el delincuente obtiene un beneficio económico como consecuencia del delito informático. Este beneficio puede consistir en el robo de dinero o de bienes, o en el cobro de un rescate.

Definición conceptual de estafa informática

El concepto de estafa informática, este concepto no lo podemos separar de la conocida estafa, entendiéndose esta como el acto de engañar a otra persona, haciéndola creer que la conducta realizada no le está causando ningún daño.

Cuando estamos hablamos de estada informática esta debe de entenderse con el uso de medios tecnológicos, ósea, el uso de aparatos electrónicos como lo puede ser celulares en el uso de

llamadas telefónicas o mensajes de texto o correos electrónicos, computadoras con la creación de páginas piratas para la captura de información, datafonos modificados, etc., son muchas las maneras en las cuales los delincuentes pueden utilizar aparatos tecnológicos para su beneficio.

Un concepto que utilizado por la doctrina para la esta informática es: “Las llamadas estafas por computador pueden definirse como toda manipulación o alteración del proceso de elaboración electrónica de cualquier clase y en cualquier momento de este, realizada con ánimo de lucro y causando un perjuicio económico de un tercero” (Flores, 2012, p.202), resalta el uso de aparatos electrónicos para cometer este delito.

Sobre el autor del delito de estafa informática, este sujeto debe de poseer conocimientos de manejo de equipos de tecnológicos, como el uso de computadoras, celulares, sumado a una astucia para engañar a sus víctimas, ese conocimiento técnico es lo que configura el tipo penal del artículo 217 bis del código penal, siendo “manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información” esto representa la parte típica del delito de estafa informática, esto porque el delito de estafa informática requiere algún manejo de programas que afecte el proceso de los datos del sistema.

Definición legal y normativa vigente

Son numerosas las definiciones que pueden ser utilizadas para definir lo que es la estafa informática, la doctrina es amplia con terminología, sin embargo todas arrojan denominativos comunes como “toda conducta fraudulenta realizadas a través de o con la ayuda de un sistema informático por medio de la cual alguien trata de obtener un beneficio ilícito” (CIJUL, s.f, p. 3), esta definición es acorde con la normativa vigente para nuestro país, siendo el concepto más preciso el que nos define el código penal en su artículo 217 bis, siendo esta:

> … 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.

Por lo tanto, la estafa informática en la legislación costarricense se define como el delito informático que se comete mediante la utilización de un sistema informático o de cualquier otro medio electrónico, informático o telemático, para obtener un beneficio económico o patrimonial, mediante engaño o defraudación.

> El Dr. Christian Hess Araya, Juez del Poder Judicial, explicó que abordar esta temática se da desde dos tendencias: la que considera los delitos informáticos conductas novedosas, donde las acciones y los tipos penales son nuevos y múltiples; y la que ve esos delitos como conductas tradicionales en un contexto moderno, para lo que se reforman o agregan leyes existentes, (UCR, 2009, párr. 3).

Los delitos de estafa informática según como lo expone el Dr. Hess, puede analizarse desde dos posiciones, como el bien lo define desde la novedad del delito o desde un contexto modernos, siendo el delito de estafa ya reconocido, lo que ocurre es una evolución del medio de para la comisión del delito, puesto la base del mismo es el engaño, el cual es el método de disuadir a la víctima para que colabore con el delincuente y facilite "información" que lo perjudique en su ámbito patrimonial.

Ante la versatilidad de internet para la comisión de delitos, el Estado como respuesta a la evolución de la estafa por medios informáticos, creo nuevos tipo penales, los cuales son una ayuda para la persona juzgadora y demás operadores del derecho ante la delincuencia informática, siendo estos integrados al código penal en la reforma del 2012 por medio de la ley 9048.

> En el caso de Costa Rica se han utilizado ambas tendencias, en una combinación de reformas y creación de tipos penales, que castigan las acciones delictivas, por ejemplo, la creación de los delitos de fraude electrónico, alteración de datos y sabotaje informático y la propuesta para reformar artículos del Código Penal, en cuanto a fraudes de tarjetas de crédito e información bancaria o el proyecto de Ley de Delitos Informáticos. (UCR, 2009, párr. 4).

Se deduce que, para que se configure el delito de estafa informática, es necesario que se cumplan los siguientes elementos:

1. Utilización de un sistema informático o de cualquier otro medio electrónico, informático o telemático. Este elemento se refiere al medio utilizado por el delincuente para cometer el delito. El medio puede ser un ordenador, un teléfono móvil, una red social, etc.
2. Engaño o defraudación. Este elemento se refiere al acto realizado por el delincuente para engañar a la víctima. El engaño puede consistir en la utilización de información falsa, la ocultación de información relevante o la utilización de técnicas de persuasión.
3. Obtención de un beneficio económico o patrimonial. Este elemento se refiere al resultado del delito. El delincuente debe obtener un beneficio económico o patrimonial, como dinero, bienes o servicios.

Como ejemplos de estafa informática que identifiquen mejor el delito pueden ser los siguientes:

1. El envío de correos electrónicos fraudulentos que inducen a la víctima a realizar una transferencia bancaria.
2. La creación de páginas web falsas que imitan a páginas web legítimas para captar datos personales o bancarios de las víctimas.
3. El uso de redes sociales para engañar a las víctimas con ofertas o promociones falsas.

La estafa informática es un delito grave que puede tener graves consecuencias para las víctimas. Las víctimas pueden sufrir pérdidas económicas importantes, así como daños a su reputación o a su privacidad.

Como parte de los delitos informáticos que se tipifican en el código penal, tenemos los siguientes:

Artículo 217 bis. - Estafa informática

Artículo 229 bis. - Daño informático.

Artículo 230.- Suplantación de identidad

Artículo 231.- Espionaje informático

Artículo 232.- Instalación o propagación de programas informáticos maliciosos

Artículo 233.- Suplantación de páginas electrónicas

Artículo 234.- Facilitación del delito informático

Artículo 235.- Narcotráfico y crimen organizado

Artículo 236.- Difusión de información falsa

La evolución de los medios informáticos

Según el desarrollo temático de este estudio, es evidente que la evolución de los medios informáticos ha tenido un gran impacto en la estafa informática. Los primeros casos de estafa informática se basaban en el uso de la tecnología para engañar a las víctimas, como el envío de correos electrónicos fraudulentos o la creación de sitios web falsos. Sin embargo, a medida que la tecnología ha avanzado, los estafadores han desarrollado nuevas técnicas más sofisticadas.

Según Parada, Ricardo Antonio, (2018, p. 5).

> La creación de internet implicó la aparición de nuevos paradigmas en materia de procesos de comunicación masiva. Por tal hito, el derecho tuvo que readecuar sus instituciones para describir, predecir y regular las conductas sociales materializadas en los procesos, mediante herramientas que permitan reglamentar aquellas conductas penalmente reprochables.

Para continuar con la evolución de los medios informáticos se toma como referencia el artículo publicado por Gustavo Sain (2018, p. 8) el cual expone que:

> Con la apertura global de internet, a mediados de los años noventa, por parte de la administración norteamericana, y el posterior desembarco de empresas y bancos a la red para el desarrollo del comercio electrónico, la industria editorial, discográfica y cinematográfica comenzó una afrenta contra la multiplicidad de casos de violaciones a los derechos de autor, a partir de la descarga e intercambio en línea de obras digitalizadas, música y películas protegidas bajo leyes de copyright. Asimismo, bajo la posibilidad de construcción de identidades ficticias que brindan los entornos virtuales en internet, un rebrote de pedofilia inundó la red mediante la distribución de imágenes de pornografía

infantil. Asimismo, el tema de la protección a la intimidad y la privacidad de las personas comenzaron a ser una preocupación a partir del uso de nuevas tecnologías digitales en la red.

Se deduce de las citas anteriores que algunos de los principales cambios en los medios informáticos que han afectado a la estafa informática son:

1. La proliferación de dispositivos móviles: Los dispositivos móviles, como los teléfonos inteligentes y las tabletas, han hecho que sea más fácil para los estafadores acceder a las víctimas desde cualquier lugar.
2. El aumento de la conectividad: La conectividad a Internet de alta velocidad ha permitido a los estafadores distribuir sus ataques a un mayor número de víctimas.
3. La sofisticación del software malicioso: El software malicioso, como los virus, los troyanos y los ransomware, se han vuelto más sofisticado y difíciles de detectar.

Estos cambios han hecho que la estafa informática sea un problema cada vez más grave. Los estafadores pueden ahora llegar a un mayor número de víctimas y causar un daño financiero más significativo. Se puede concluir que, de la evolución de los medios informáticos en la estafa informática, se podrían considerar los siguientes aspectos más sobresalientes:

1. Los principales cambios en los medios informáticos que han afectado a la estafa informática.
2. Cómo estos cambios han facilitado a los estafadores el acceso a las víctimas y
3. El daño financiero y los desafíos que estos cambios plantean en la lucha contra la estafa informática.

El impacto social de la ciberdelincuencia

Los países emergentes o en vías de desarrollo, presentan también unas condiciones particulares que permiten entender el crecimiento del *e-commerce* o comercio electrónico que consiste en la distribución, venta, compra, marketing y suministro de información de productos o servicios a través de Internet.

Tanto es así que Tavera y Londoño (2014, p.214) afirman que:

> En el caso de los mercados emergentes, las altas tasas de penetración de Internet conllevan a que los usuarios se sientan más cómodos con el uso de las plataformas de comercio electrónico dado que su uso no difiere significativamente de la forma de navegación por la Web, lo que puede explicar la no relación entre la facilidad percibida de uso como antecedente explicativo de la formación de actitudes hacia el comercio electrónico.

En este sentido, es posible reconocer que hay una estrecha relación entre las posibilidades de conexión a internet y el crecimiento del comercio electrónico, y este crecimiento en cobertura de internet ha sido uno de los principales enfoques de dichos países emergentes, ya que, potenciando este aspecto, es más posible insertar su economía en circuitos internacionales que sean provechosos.

Sin embargo, el comercio electrónico según la Organización para la Cooperación y el Desarrollo Económicos (OCDE- 2019), se refiere a:

> La venta o compra de bienes o servicios que se realiza a través de redes informáticas con métodos específicamente diseñados para recibir o colocar pedidos; para determinar si una transacción comercial se puede considerar como comercio electrónico se toma en cuenta el método de pedido y no las características del producto que se adquiere, las partes implicadas, el método de pago o el canal de entrega (p. 17)

En este apartado de la investigación se trata acerca de la ciberdelincuencia, como un tipo de delito que afecta a la sociedad en la actualidad debido a los avances tecnológicos y la poca costumbre de revisar o eliminar la información de las cuentas de banco, dejar de aceptar a todas las personas que no conoce en las redes sociales y no abrir todos los correos electrónicos que reciben porque pueden tener virus. Si no se toman las precauciones adecuadas se deja una puerta abierta para que cualquier persona con un conocimiento de ciertos programas o mediante el uso de virus pueden engañar para tener acceso a la información personal y financiera, pasando a ser víctimas de estos delincuentes. Se debe considerar que, mediante el uso indebido de la tecnología, los delincuentes cibernéticos pueden llevar a las empresas a la ruina e incluso arruinar la vida a las personas. Muchos países y organizaciones de todo el mundo luchan para poner un alto a los

delincuentes cibernéticos y contribuir a la seguridad de los sistemas. Considerando que el impacto social de la ciberdelincuencia es un tema complejo que abarca una amplia gama de aspectos.

De acuerdo con Gil López Isabel, Fresneda Saldarriaga y Molina Grajales (2021, pp. 32-33) en su obra “Impacto económico y social que ha generado el delito cibernético sobre el comercio electrónico en Colombia durante el periodo 2019-2021” se justifica establecer algunos de los impactos más relevantes, los cuales son:

Impacto económico: La ciberdelincuencia tiene un impacto económico significativo en la sociedad, tanto a nivel individual como global. Los ciberdelincuentes pueden robar dinero, datos, o información confidencial, lo que puede causar pérdidas económicas significativas a las víctimas. Según el informe "*The Global Economic Impact of Cybercrime"* de la firma de ciberseguridad “Cybersecurity Ventures”, el costo mundial de la ciberdelincuencia en 2022 fue de 6 billones de dólares, y se espera que alcance los 10,5 billones de dólares en 2025.

Impacto en la seguridad: La ciberdelincuencia también tiene un impacto en la seguridad de las personas y las organizaciones. Los ciberdelincuentes pueden usar su acceso a sistemas informáticos para robar información personal, chantajear a las víctimas, o incluso causar daños físicos. Por ejemplo, en 2021, un ataque cibernético a la empresa Colonial Pipeline provocó el cierre de un importante oleoducto en Estados Unidos, lo que llevó a una escasez de gasolina en el país.

Impacto en la privacidad: La ciberdelincuencia puede poner en riesgo la privacidad de las personas. Los ciberdelincuentes pueden robar datos personales, como números de tarjetas de crédito, direcciones de correo electrónico, o contraseñas. Esta información puede usarse para cometer otros delitos, como el fraude o el robo de identidad.

Impacto en la confianza: La ciberdelincuencia puede erosionar la confianza en las instituciones y las tecnologías digitales. Las personas pueden sentir miedo de usar Internet o las redes sociales si creen que sus datos están en riesgo. Esto puede tener un impacto negativo en la economía y la sociedad en general.

Impacto en los derechos humanos: La ciberdelincuencia también puede violar los derechos humanos. Por ejemplo, el ciber acoso puede causar angustia emocional a las víctimas, y el ciber terrorismo puede restringir la libertad de expresión.

Además de estos aspectos, también es importante considerar el impacto social de la ciberdelincuencia en términos de género, raza, o nivel socioeconómico. Por ejemplo, las mujeres y las personas de minorías son más propensas a ser víctimas de ciber acoso, y las personas de bajos ingresos pueden tener menos acceso a las herramientas y los recursos necesarios para protegerse de la ciberdelincuencia. Al respecto**, e**s importante que las instituciones públicas, las empresas, y los individuos tomen medidas para mitigar el impacto social de la ciberdelincuencia. Estas medidas pueden incluir la educación sobre la ciberseguridad, la inversión en tecnologías de seguridad, y la cooperación internacional para combatir la ciberdelincuencia.

La necesidad de una respuesta penal eficaz

El derecho penal se considera la última ratio por ser la respuesta ante la inobservancia del ciudadano que infringe las reglas de convivencia social, propiamente en el caso de los ciberdelitos, es una delincuencia en la que los autores son sujetos con conocimientos y formación en ramas de la ingeniería como son los sistemas de computadora, siendo esto un reto para el derecho penal, porque conlleva un reto al Misterio Público y al OIJ, en el sentido que ante un delincuente con dominio en los sistemas de software la persona investigadora si no es un experto en informática, puede suceder que no posea el conocimiento técnico sobre como encausar una investigación a nivel de software para la ubicación del ciberdelincuente.

Lo mismo ocurre con las llamadas telefónicas, que ante el poco control de los proveedores del servicio las líneas se expiden a personas sin ningún tipo de registro para ubicar al dueño del servicio, con las direcciones IP existe software que permite fácilmente manipular la información de la IP en cuanto a identificación y ubicación.

Ante estos retos surge la necesidad de una repuesta penal que le permita al sistema de justicia brindar una respuesta positiva a la víctima, respuesta que actualmente no es eficaz en la identificación del delincuente informático.

De acuerdo con López Gorostidi (2020) es necesario realizar un examen que se cuestione si la respuesta penal actual a este tipo de delitos cibernéticos es adecuada en términos de proporcionalidad entre el daño causado y la pena aparejada a cada delito. Y señala que, una respuesta penal eficaz ante el impacto social de la ciberdelincuencia debe tener en cuenta los siguientes aspectos:

1. La naturaleza de la ciberdelincuencia: La ciberdelincuencia es un delito que se comete en el espacio cibernético, lo que plantea desafíos únicos para la persecución penal. Por ejemplo, es difícil identificar a los autores de ciberdelitos, y es posible que los delitos se cometan en jurisdicciones diferentes.
2. El impacto social de la ciberdelincuencia: La ciberdelincuencia puede tener un impacto significativo en la sociedad, causando daños económicos, psicológicos y sociales. Por ejemplo, la ciberdelincuencia puede provocar pérdidas económicas, daños a la reputación y la angustia psicológica. (p. 221)

Como complemento de lo expuesto anteriormente López Gorostidi indica que los objetivos de la respuesta penal deben tener como objetivo disuadir a los delincuentes, proteger a las víctimas y reparar el daño causado.

Y agrega que se pueden identificar una serie de medidas que podrían formar parte de una respuesta penal eficaz a la ciberdelincuencia:

1. Reforma legislativa: La legislación penal debe actualizarse para reflejar la naturaleza cambiante de la ciberdelincuencia. Por ejemplo, es necesario ampliar el alcance de las leyes penales para incluir nuevas formas de ciberdelincuencia, como el ciberespionaje y el ciberterrorismo.
2. Fortalecimiento de las capacidades de investigación y persecución: Las autoridades encargadas de hacer cumplir la ley deben tener las capacidades necesarias para investigar y perseguir los ciberdelitos. Esto incluye el acceso a la tecnología forense, la formación especializada y la cooperación internacional.
3. Educación y concienciación: La educación y la concienciación pública sobre la ciberdelincuencia pueden ayudar a reducir la vulnerabilidad de las personas y las organizaciones a las ciber amenazas. (López Gorostidi,2020, p.224)

Si el sistema penal de justicia mejora sus condiciones de persecución, esto ayudaría a disuadir al delincuente de estafa informática, como parte de las soluciones, indudablemente la educación es una herramienta que permitiría la disminución de este tipo de delitos, si se brinda educación en los centros escolares, campañas de concientización sobre métodos de estafa, la ciudadanía tendría herramientas para no ser víctimas de los delincuentes que se valen de la tecnología y del descuido de las personas para cometer el delito.

La inversión en herramientas tecnológicas de corte investigativo son una necesidad del Poder Judicial, en un mundo donde las herramientas tecnológicas son de uso diario por los delincuentes, resulta imperioso que el ente de persecución cuente con herramientas que permitan el rastreo de una huella digital para tratar de localizar a los delincuentes.

Aspectos técnicos de la estafa informática

La estafa informática se estructura de diferentes elementos para que esta pueda ser ejecutada, siendo su característica principal el uso de aparatos tecnológicos para cometer el engaño, estos aparatos deben de poseer una conexión internet que les permita comunicarse con otros dispositivos, siendo estos los de las víctimas escogidas por el delincuente o en su defecto las victimas al azar.

> … respecto de la del fraude informático, que tiene varios componentes especializantes, como lo son, que debe cometerse utilizando un sistema de cómputo; por medio de la manipulación de la información que esté codificada, o sistematizada en aquel; y bajo un determinado programa de informática. (CIJUL, 2023, p. 17).

Para que el delito de estafa informática surja como tal, debe de cometerse valiéndose de la tecnología por parte del delincuente, la tecnología usada por el delincuente no es necesariamente una computadora, lo que exige la norma es que se valga de aparatos tecnológicos que le facilite la manipulación de la información de la víctima, a lo cual el internet siempre estará presente como medio primordial para la comisión del delito, dentro de los dispositivos más comunes para la ejecución del engaño en la estafa informática se encuentran las computadoras y teléfonos, esto por la facilidad de para obtenerlos, también existe dispositivos más elaborados para obtener

información como los capturadores de códigos a distancia, los copiadores de la bandas magnéticas de las tarjetas de crédito o debido.

> En otro sentido señala Camacho Losa, que el fraude informático lo configura como el bloque de la delincuencia informática integrado por usos indebidos o manipulaciones fraudulentas de elementos informáticos de cualquier tipo (hardware, software, líneas de comunicación, información mecanizada, etc., que posibilitan un benéfico ilícito" (CIJUL, s.f, p. 3)

El internet abre una posibilidad al alcance de la tecnología tanto para delinquir como para evitar los delitos, los ingenieros en sistema elaboran maquinas o dispositivos que se utilizan facilitar las labores de los seres humanos, estos dispositivos funcionan a través de programas o software, los cuales son los que dan la funcionabilidad de los dispositivos.

Ejemplo de ello son las computadoras en los bancos, donde la maquina se utiliza para digitar los números que representan el dinero, es a través del software que le permite al digitador realizar los movimientos del dinero que el cliente desea, como pagar servicios, retirar dinero, transferencias, etc., este principio de uso es el mismo que utilizan los hackers para delinquir, dispositivos con programas.

> … respecto de la del fraude informático, que tiene varios componentes especializantes, como lo son, que debe cometerse utilizando un sistema de cómputo; por medio de la manipulación de la información que esté codificada, o sistematizada en aquel; y bajo un determinado programa de informática. (CIJUL, 2023, p. 17).

Como componentes del delito de estafa informática se debe de reconocer que como elemento material para cometer el delito es indispensable el uso de algún dispositivo tecnológico, sin eso es imposible la comisión del delito, puesto sino estaríamos ante una estafa pura y simple, algunos conceptos importantes de comprender son los siguientes:

1. Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.
2. Hardware: conjunto de aparatos de una computadora

Estos dos conceptos son la base de cualquier delito de estafa informática, donde intervienen calidad, tecnología, diseño, componentes, programas especializados, etc., infinidad de posibilidades para el delincuente y el ente encargado de proteger los datos.

Como medios utilizados con mayor frecuencia para la ejecución de la estafa informática se pueden mencionar: correos electrónicos, malware, hacking, falsificación de documentos electrónicos, llamadas telefónicas.

Ingeniería Social

Existen diferentes métodos para cometer los delitos informáticos, siendo estos por expertos de un alto grado de conocimiento en informática, que valiéndose de su conocimiento en programación hacen ingreso a computadoras ajenas sin que el usuario se entere, todo a través de programas informáticos, y también existen los delincuentes que se valen del descuido de las víctimas, valiéndose de técnicas de interacción para hacerse conseguir de información como lo son claves de páginas bancarias, siendo esta técnica denominada por la doctrina como ingeniería social.

> Se ha adoptado el término ingeniería social para referirse al conjunto de técnicas empleadas por intrusos, con el fin de extraer información sensible de los usuarios de un sistema informático. entre todas las técnicas cabe destacar las siguientes: A) intrusos que se hacen pasar por empleados de otros departamentos de la empresa, por personal de un proveedor de servicios de informática, de un operador de telefonía o de acceso a internet; B) correos electrónicos que suplantan la identidad de otra persona u organización o que incluyen textos o ficheros adjuntos a modo de reclamo; C) usuarios que utilizan foros y chats en internet para conseguir tener acceso a determinados ficheros sensibles del sistema o a información referente a la configuración y medidas de protección de los equipos; D) shoulder surfing: Cuestionaste los usuarios pero obtener nombre de usuarios y contraseñas, mediante la observación directa de lo que tecleen; E) dumpster diving (“basurero”): Revisión de los papeles y documentos que se tiran a la basura y no son destruidos de forma segura; F) Puesta en marcha de websites maliciosos que tratan de engañar a sus usuarios; G) redes sociales. en este caso en particular se da mediante los mensajes y post, es decir, los links donde se fue redirigir al usuario alguna foto o video (por ejemplo) accediendo directamente a un

> código malicioso, también es el caso de los hoax que podemos encontrarlos en noticias falsas con contenido engañoso, propagandas para distribuirse en cadena debido a que emplean temáticas impactantes o sensacionalistas que aparentan venir de una fuente confiable, (Nava, 2019, p.130).

Se puede definir la ingeniería social como un conjunto de técnicas sociales, las cuales son usadas de forma consciente y premeditada para la obtención de información de terceros, es decir, es el aprovechamiento de los conocimientos de determinadas personas para convencer a otras de que ejecuten acciones o actos que puedan revelar información, esto sin la necesidad de hacer uso de herramientas ajenas al contacto directo con la persona. como característica esencial, un ataque de ingeniería social de su éxito a fallas humanas, hoy por falta de procedimientos internos eficaces, normalmente asociado a la falta de clasificación de la información y a la capacitación del personal sobre la base de dicha clasificación y sus cuidados, vas a su éxito en que las personas somos predecibles y tendemos a reaccionar de cierto modo al enfrentarnos a determinadas situaciones, (Nava, 2019).

Vishing

Los delincuentes utilizan diferentes métodos de aplicar la ingeniería social, una de las más comunes es la llamada telefónica, en donde el delincuente pretende obtener información de accesos a cuentas bancarias para realizar las transferencias fraudulentas del dinero de las víctimas.

> El Vishing es un tipo de estafa ingeniería social por teléfono en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la vida. (Ribón, 2024, p.42).

El modo de operación de este tipo de ingeniería social, es la realización de una llamada a una a la víctima, en la que se identifica como una persona de una entidad bancaria, municipalidad o prestadora de servicios, en la cual la víctima es cliente, dónde lo solicitan datos personales sensibles con la pretendida excusa de algún tipo de verificación o incluso el acceso remoto a alguno de sus dispositivos, para lograr una confianza con la víctima, el delincuente recaba información previa sobre ella, de esta forma engañando a la víctima induciéndola a error bajo una falsa confianza, el delincuente una vez que obtiene la confianza de la víctima de manera audaz logra que

la víctima le brinde los datos de acceso a su cuenta bancaria, para posteriormente realizar el traslado de los dineros.

Phishing

El phishing, es otro método por el cual los ciberdelincuentes logran despojar a sus víctimas de su patrimonio, conocido como el delito como “pescar”, esto porque los ciberdelincuentes a través de las plataformas tecnológicas tiran el mensaje y esperan a ver quien caiga.

> El dominado Phishing puede definirse como “la pesca de datos” que tienen como objetivo provocar de un daño patrimonial a tercero, sin su consentimiento, mediante la utilización fraudulenta de sus claves. como expone PIQUERES CASTELLOTE consiste en la captación ilícita de datos personales, principalmente relacionados con claves para el acceso a servicios bancarios y financieros a través de correos electrónicos o páginas web que imitan y copian la imagen o apariencia de una entidad bancaria o financiera. Esta captura ajena de datos se realiza pues, por la común, mediante técnicas engañosas que generan la confianza necesaria en el afectado para la cesación o facilitación de sus datos, por lo común a través de correos electrónicos, mensajería móvil, redes sociales o llamadas telefónicas, (Ribón, 2024, p.31).

El ciberdelincuente, a través de la ingeniería social como tipología delictiva, utiliza el phishing como medio para realizar la estafa informática, en el caso de esta forma de cometer el delito, el ciberdelincuente de una manera muy audaz genera contenido de aparente confianza a la víctima y de esta forma gana su confianza, con lo cual accede a sus cuentas bancarias que la ayuda de la misma víctima, con el entendido que la víctima lo hace bajo un error y pensando que está siendo ayudada.

Correos electrónicos fraudulentos

Estos constituyen los correos que recibimos suplantando la identidad de personas u organizaciones que tienen alguna relación con nosotros y cuyo objetivo es sustraernos información personal.

El Poder Judicial de Misiones Argentina de la Secretaría Tecnología Informática indica en su publicación “Como detectar y protegernos, consejos y estrategias” (2019, p. 1 - 2).

1. El dominio de la dirección de email no coincide con el de la empresa Esto ocurre en todos los correos electrónicos falsos (emails de phishing). Estos emails se envían desde direcciones de correo que no tienen nada que ver con la empresa a la que están intentado suplantar.
2. Faltas de ortografía o de concordancia, cuando ves un email lleno de faltas de ortografía, con errores y faltas de concordancia, ¡sospecha! Es una señal de que este correo electrónico puede ser falso.
3. El correo solicita información personal, normalmente los correos electrónicos falsos tratan de recopilar información personal o de pago con el objetivo de hacer un uso inadecuado de ella. Para obtener estos datos, normalmente te piden que verifiques una cuenta, que actualices tu información, tu número de cuenta, etc.
4. El asunto del correo es de máxima alerta, otra señal que te indica que estás ante un correo electrónico falso es el asunto. ¿Te indican que acabas de ganar 100,000$? ¿Van a cancelar tu cuenta bancaria? Recordó que cuando tienes contratado un servicio y está próximo a vencer, las empresas siempre suelen enviar varios recordatorios.
5. Archivos adjuntos Otra de las características de los correos electrónicos falsos es que la gran mayoría incluyen siempre archivos adjuntos para evitar que estos emails acaben en la bandeja de spam. Pero, peor aún, en muchos casos, estos archivos adjuntos no son únicamente para engañar a los gestores de correo, sino que se utilizan para inyectar malware e infectar tu equipo.

Para no ser víctima de un ciberataque y proteger tu vida online, recuerda tener una serie de precauciones:

1. No abras correos de usuarios desconocidos, de empresas en las que no tienes una cuenta o correos con asuntos muy alarmantes. Lo más probable es que se trate de un correo electrónico falso.
2. Mucho cuidado con los archivos adjuntos. Si no conoces la dirección de la persona que te lo envía, mejor no lo abras.

3. ¿Te están solicitando actualizar información? Hazlo siempre desde la página oficial y no desde el correo. Si tienes una cuenta en una empresa, tendrás acceso a un área en la que puedas realizar todas estas gestiones sin necesidad de acceder a través de un enlace sospechoso.
4. desconfía de los mensajes alarmantes. Es muy raro que una empresa te solicite datos personales o de pago por email

Cualquier usuario puede ser víctima de un ataque si no tiene en cuenta algunas de las medidas que acabamos de ver en este post. Detectar correos electrónicos falsos es relativamente fácil, pero nadie está a salvo de caer en una estafa o ser víctima de un ataque de phishing.

Malware

Como parte de los Software, se encuentran los malicious software o softwares maliciosos, los cuales son programas para sistemas operativos, que su función es ingresar al dispositivo y realizar diferentes funciones según sea su programación, como robar datos, limitando accesos, instalar más malware, etc.

> El malware es un software o código informático diseñado para infectar, dañar o acceder a sistemas informáticos. Hay diferentes tipos de malware, y cada uno infecta o corrompe dispositivos de forma distinta, pero todas las variantes de malware están diseñadas para poner en peligro la seguridad y privacidad de los sistemas informáticos, (Belcic, 2023, párr. 2).

Dentro del estudio es la segunda acción de ataque más importante. Malware es cualquier software o código cuyo objetivo es comprometer o dañar los activos de información sin el consentimiento del propietario

Hacking

El Hacking es probablemente la forma más popular de reconocer una estafa informática, esto porque el concepto de pirata informático es reconocido mundialmente, “El ejemplo clásico de un hacker es un cibercriminal que explota vulnerabilidades de seguridad o supera las medidas de

seguridad para irrumpir en una computadora o red informática y robar datos" (IBM, s.f, párr. 1), esta es la definición que tenemos los usuarios de computadoras, la de una persona al otro lado del mundo con una gran destreza para ingresar a nuestra computadora y obtener nuestra información.

En la legislación costarricense, se adiciono en el año 2012 la sección de delitos informáticos y conexos, siendo tipificados los delitos del artículo 230 al 236, y reformados los artículos 196 bis, 217 bis y 229 bis, con esta reforma el legislador brinda una respuesta punitivista ante los delitos informáticos crecientes en el país.

Existe un reto importante en determinar al autor de los delitos informáticos, el cual es la localización del autor la persona delincuente, la característica principal es el anonimato con el que se actúa, esto porque lo hacen a través de una computadora con una conexión IP en cualquier parte del mundo, desde que se comete el delito surgen varias interrogantes para la localización del delincuente, como, por ejemplo:

1. Cuál es la dirección IP de la computadora con la que se cometió el delito
2. Es la computadora conectada a la IP la que se utilizó para el delito
3. Es la persona dueña de la computadora la que cometió el delito

Como estas y otras muchas preguntas surgen a los operadores del derecho cuando se está al frente de un delito informático.

Falsificación de documentos electrónicos

En Costa Rica es a partir del 2005 que se regula con la ley N° 8454 el uso de documentos electrónicos, esto con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, donde se regula principalmente la migración del papel tradicional a documentos de soporte electrónico como documentos PDF.

La ley 8454 en su artículo 3 indica:

> Reconocimiento de la equivalencia funcional. Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.

> En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. No obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular.

De esta ley se desprende que con la globalización a través del internet se interrumpa las fronteras y el mercado se dinamice, venciendo la barrera de la distancia para ejecutar negocios, es claro lo positivo de esta forma de emitir documentos, reduciendo tiempo y gastos para transportarse a firmar documentos en papel.

Como una variante importante sobre el tema de estudio, se debe de saber que a cómo es posible la falsificación de documentos físicos, lo es igual a documentos digitales, lo cual puede ocurrir para realizar estafas informáticas.

Los documentos electrónicos son válidos con la firma digital, la cual se integra al documento por medio de un software que con una contraseña solo conocida por el usuario se integra al documento, esa contraseña en principio no puede ser conocida por ninguna otra persona.

Como medidas de seguridad a los documentos electrónicos se puede mencionar la criptografía, “es la ciencia que trata el enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente” (Jovel, s.f, p. 41), esta medida de seguridad permite solo a los usuarios autorizados el observar la información del documento, dando con ello seguridad.

Otra medida de seguridad que se complementa con la criptografía es la firma digital, la cual se integra al documento electrónico con por medio de un software.

> La firma digital puede consistir en cifras, signos, códigos, claves, etc., lo cierto es que se considera que puede ser más confiable que la ológrafa, por el hecho de que esta última es siempre irregular y por consiguiente de difícil verificación visual, ya sabemos que para determinar su autencidad de manera confiable debe acudirse a peritos en grafología, (Jovel, s.f, p. 43).

A pesar de la seguridad que puede presentar la firma digital, esta puede ser eventualmente estar sujeta a manipulación o falsificaciones de algún tipo, sea este por un descuido del usuario en brindar su contraseña, perder su tarjeta, que le copien una imagen de la firma de un documento anterior y no sea verificado por la contraparte.

Estrategias para superar los retos de la individualización

La cooperación internacional

Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001), como herramienta principal para los delitos cibernéticos, Costa Rica de adhiere en julio de 2017 al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001), este convenio surge de la innegable preocupación por los delitos informáticos, donde la brecha de las fronteras es superada fácilmente por los autores de los delitos informáticos, el convenio pretende una cooperación en materia penal, donde la ayuda de los estados partes sea de una comisión efectiva para la captura de los posibles autores, así como la ayuda necesaria para la facilidad de la investigación.

El convenio de Budapest tiene una antesala a nivel de comunidad internacional, (Nava, 2019), con la existencia del internet para finales del siglo XX, surgen los primeros ciberdelitos, es por ello que varias organizaciones mundiales como: Naciones Unidas, G-8, Unión Europea y el consejo de Europa, dimensionan el peligro de internet en cuanto a su finalidad como medio para cometer delitos, es por esta potencialidad que en 1981 se realizó el Consejo de Europa para la protección de personas con respecto al tratamiento informatizado de los datos personales, el objetivo del mencionado convenio era atribuirle penas a la violación de datos personales, datos que permiten ocultarse a través de una identidad falsa para cometer delitos.

Para 1997, el Gobierno del Consejo de Europa propone un plan para combatir la ciberdelincuencia, en esta ocasión el bloque de países convino la penalización y prevención de los delitos informáticos, con el fundamento de la protección de datos y lucha contra el fraude, con ello podemos deducir que el uso del internet para cometer delitos aumento, como el robo de identidad para cometer delitos y el uso de programas de MALWARE para el mismo fin.

En el 2001, se crea el primer cuerpo normativo que tipifico los delitos informáticos, esto fue producto de la Convención Europea sobre el delito informático, como la finalidad de toda norma es regular, con la creación de este cuerpo normativo se identifica que los ciberdelincuente no poseen fronteras, por lo que se debió crear una norma de aplicación internacional para tipificar lo que se consideraría delito o no en cada país miembro.

La mayor herramienta a nivel internacional para el combate de la ciberdelincuencia es el Convenio de Europa sobre Ciberdelincuencia, el cual es un compendio o guía legal que deben de implementar los países adherentes al mismo con el fin de penalizar conductas cibercriminales en las leyes sustantivas de cada país.

El convenio de Budapest, ofrece una serie de principios a ejecutar para cuando se esté al frente de un ciberdelito, todo con el fin de facilitar la investigación de los ciberdelitos, obtención y custodia de prueba, apoyo de agentes de policía o similares, en forma general es ayudar a compartir información para resolver al país interesado a resolver el ciberataque.

La comunidad internacional reconoce en 2007, los delitos informáticos como fraudes, los cuales son cometidos utilizando como medio la manipulación de computadoras, siendo la manipulación de datos de entrada, programas, falsificaciones, daños, modificaciones, sabotaje informático, accesos no autorizados, hackers, entre otros.

Este convenio vincula a la materia penal en cada uno de los países, estableciendo herramientas legales que permitan una política de persecución penal en los delitos que utilizan como medio un dispositivo electrónico, los países miembros se comprometen a la homologación del derecho penal sustantivo y procesal, así como una rápida cooperación internacional ante una solicitud.

Convenio de NASSAU, es un Convenio de la Organización de los Estados Americanos, la importancia de este convenio radica en que los “Estados parte se prestarán asistencia mutua en investigaciones, juicios y actuaciones en materia penal referentes a delitos cuyo conocimiento sea competencia del Estado requirente al momento de solicitar la asistencia” (Convención de Nassau, 2011, art. 2). Eso es de vital importancia en materia penal, Puesto, permite a los Estados que requieran una investigación de delitos informáticos, solicitar la colaboración, en temas de investigación con la policía especializada del otro país.

La principal forma de asistencia, tras la solicitud de ayuda de un país será la investigación o enjuiciamiento de delitos que el país solicitante requiera el, siendo en este caso, que para el delito de estafa informática donde se logre identificar a un autor de este, se podrá solicitar colaboración en cuanto a la investigación, obtención de prueba, custodia de esta, para posteriormente ser trasladada, o en su defecto realizar el juicio en el país del delincuente.

La asistencia prevista en esta Convención comprenderá, entre otros, los siguientes actos:

a. notificación de resoluciones y sentencias;

b. recepción de testimonios y declaraciones de personas;

c. notificación de testigos y peritos a fin de que rindan testimonio;

d. práctica de embargo y secuestro de bienes, inmovilización de activos y asistencia en procedimientos relativos a la incautación;

e. efectuar inspecciones o incautaciones;

f. examinar objetos y lugares;

g. exhibir documentos judiciales;

h. remisión de documentos, informes, información y elementos de prueba;

i. el traslado de personas detenidas, a los efectos de la presente Convención, y

j. cualquier otro acto siempre que hubiere acuerdo entre el Estado requirente y el Estado requerido. (Convención de Nassau, 2011, art. 7).

Este convenio tiene una gran relevancia para el delito de estafa informática, puesto este es un delito penal, y aunque existe el convenio de Budapest, el convenio de asistencia mutua en materia penal (NASSAU) complementa todo el tema de la cooperación internacional para lograr un adecuado abordaje a los delitos informáticos, incluyendo claro está la estafa informática.

Interpol, es una policía a nivel mundial de la cual se asocian distintas policías a nivel mundial con el fin de obtener una ayuda internacional, como, por ejemplo; investigaciones, capacitación, ayuda técnica, dice: “Estos conocimientos especializados sirven de apoyo a las iniciativas nacionales de lucha contra la delincuencia en cuatro áreas globales que consideramos

las más acuciantes actualmente: terrorismo, ciberdelincuencia, delincuencia organizada. y delincuencia financiera y corrupción" (INTERPOL, 2024, párr. 10), siendo el tema de interés la ciberdelincuencia, al ser INTERPOL de ámbito internacional bajo las reglas del derecho público, presenta una ayuda invaluable para Costa Rica en la colaboración para los ciberdelitos.

De lo expuesto hasta el momento se tiene claro que la ciberdelincuencia es un problema mundial creciente. Ya sea que la persona dirija una pequeña empresa o una gran compañía o que se esté adquiriendo su primer teléfono inteligente se debe tener consciencia de la ciberdelincuencia, la internet ha demostrado que ofrece oportunidades educativas y económicas que superan cualquier cosa antes vista. Esta misma herramienta, permiten la oportunidad de causar daños. Mediante el uso indebido de la tecnología, los delincuentes cibernéticos pueden llevar a las empresas a la ruina e incluso arruinar la vida a las personas. Muchos países y organizaciones de todo el mundo luchan para poner un alto a los delincuentes cibernéticos y contribuir a la seguridad de los sistemas.

La Oficina de la Naciones Unidas contra la Droga la Delincuencia (2018) ha establecido Mecanismos formales de cooperación internacional y al respeto considera:

> La cooperación internacional depende de leyes nacionales sustantivas sobre delitos cibernéticos armonizadas, que penalizan el delito cibernético, y de las leyes nacionales procesales sobre delitos cibernéticos que establecen las normas que rigen la práctica de la prueba y los procedimientos penales (discutido en Delitos Cibernéticos Módulo 3; Marcos Jurídicos y Derechos Humanos).
>
> También se puede facilitar la cooperación internacional armonizando, donde sea necesario, los instrumentos bilaterales, regionales y multilaterales sobre delitos cibernéticos. Igualmente, es necesario adherirse o ratificar los instrumentos regionales y multilaterales sobre delitos cibernéticos para hacer que sean jurídicamente vinculantes. Para más información sobre la cooperación internacional para combatir la delincuencia organizada transnacional, conviene consultar la serie de módulos universitarios sobre Delincuencia Organizada (especialmente el Módulo 11 Cooperación Internacional para Combatir la Delincuencia Organizada Internacional, (ONU, 2018).

Además, La Oficina de la Naciones Unidas contra la Droga la Delincuencia (2018) hace énfasis en que:

> La cooperación internacional se facilita con tratados bilaterales, regionales y multilaterales sobre delitos cibernéticos siempre y cuando exista una doble incriminación (es decir, una cláusula en los tratados que exija que la conducta alegada se considere ilegal en los países cooperantes). Sin la doble incriminación y sin leyes armonizadas, se crean refugios seguros para los delitos cibernéticos en los que no se puede procesar a los autores del delito. Esto se observó en el caso del virus Love Bug del año 2000, cuyo creador y distribuidor no pudo ser procesado porque sus actos no se consideraban delito en su país (Filipinas) en el momento del incidente.

En el apartado 2 del artículo 43, de la Convención de las Naciones Unidas contra la Delincuencia Organizada (2003) se señala:

> La cooperación internacional puede seguir siendo posible incluso sin una interpretación estricta del requisito de la doble incriminación. Además, «cuando la doble incriminación se considera un requisito, se estimará cumplida independientemente de si las leyes del Estado parte requerido lo incluye en la misma categoría de delitos o lo denomine con la misma terminología del Estado parte requirente si la conducta que subyace al delito por el que se solicita asistencia es un delito penal según las leyes de ambos Estados parte»

Señala la publicación Oficina de la Naciones Unidas (bis) que se presentan excepciones para el requisito de la doble incriminación. Por ejemplo, el apartado 3 del artículo 29 del Convenio sobre Delitos Cibernéticos de 2001 del Consejo de Europa no exige la doble incriminación para la «conservación rápida de datos informáticos almacenados» «por medio de un sistema informático, situado en el territorio de la otra Parte, en cuanto la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua para el registro o un acceso similar, para la incautación o un aseguramiento similar, o para la divulgación de los datos» en casos de delitos sustantivos incluidos en el presente Convenio (artículos 2 a 11).

El apartado 4 del artículo 29 establece el derecho de los estados a rechazar las solicitudes de conservación si requieren de la doble incriminación para la asistencia mutua por delitos que no están incluidos en el Convenio.

> Además de la doble incriminación, otro requisito sustantivo para la cooperación internacional es que se respeten las obligaciones internacionales en asuntos de derechos

> humanos Se pueden rechazar las solicitudes de cooperación internacional si la solicitud tiene como resultado que el Estado viole sus obligaciones internacionales en asuntos de derechos humanos al responder a la solicitud. (UNODC, 2013, pág. 205).

Interesa destacar que Oficina de la Naciones Unidas contra la Droga la Delincuencia (2018) señala que:

> Los mecanismos formales para la cooperación internacional incluyen tratados bilaterales, regionales y multilaterales sobre delitos cibernéticos. De hecho, la cooperación considera de manera preponderante estos tratados. Por ejemplo, el Acuerdo sobre Cooperación para Combatir Delitos Informáticos de la Comunidad de Estados Independientes del 2001 incluye varios artículos dedicados a la cooperación internacional (artículos 5-7), que abarcan los tipos de cooperación incluidos en el presente Acuerdo.

Es decir, intercambio de información, prestación de asistencia jurídica de conformidad con los instrumentos internacionales, y prevención, detección, represión e investigación de los delitos cibernéticos, por citar algunos, así como la manera en que los Estados Miembros pueden solicitar asistencia y las directrices sobre cómo ejecutar estas solicitudes.

El artículo 8 de este Acuerdo incluye las circunstancias en las que se puede denegar una solicitud de asistencia (es decir, cuando la solicitud infringe la legislación nacional del Estado) y el requisito de notificar por escrito al Estado requirente que su solicitud fue denegada y las razones por las que se denegó.

Lo anterior evidencia las posibles dificultades que se presentan para la necesaria individualización del delincuente informático en el ámbito internacional, sin embargo, cabe destacar que el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Pruebas en materia de Delitos Cibernéticos, también busca promover la cooperación entre los signatarios con respecto a la recopilación de pruebas y su conservación en casos de delitos cibernéticos.

En el caso concreto de solicitud de asistencia mutua se deben presentar por escrito (consulte la figura 1, en la que se muestra una solicitud de MLAT entre un país de la Unión Europea y un país que no pertenece a la UE)

> La solicitud debe incluir información sobre la autoridad requirente, el motivo de la solicitud, la descripción de la solicitud, la investigación o los procedimientos judiciales a la que se refiere la solicitud de asistencia, la descripción del delito o delitos y las leyes infringidas, toda solicitud relativa a los procedimientos a seguir para obtener, conservar y, por último, transferir las pruebas físicas y digitales (discutido en Delitos Cibernéticos Módulo 4: Introducción al Análisis Forense Digital) a la autoridad requirente, los plazos para las solicitudes de conservación de datos y para ejecutarlas, y cualquier otra información que ayude al Estado que recibe la solicitud a realizarla (consulte, por ejemplo, el artículo 5 del Convenio de Asistencia Judicial en Materia Penal de 1992 de la Comunidad Económica de los Estados de África Occidental o ECOWAS). (UNODC, 2013, p. 207).

Finalmente es necesario señalar que las solicitudes de asistencia mutua se pueden negar en ciertas circunstancias como la que se transcribe a continuación:

> Por ejemplo, si la solicitud «perjudica la soberanía, la seguridad y el orden público» (artículo 4 del Convenio de Asistencia Judicial en Materia Penal del ECOWAS; consulte también el artículo 2 del Convenio Europeo de Asistencia Judicial en Materia Penal de 1959, el apartado 4 del artículo 25 del Convenio sobre Delitos Cibernéticos del Consejo de Europa y el artículo 18 de la Ley N° 09-04 de Argelia del 14 de Shaabán de 1430 que corresponde al 5 de agosto de 2009, el cual contiene normas específicas sobre la prevención y la lucha contra los delitos relacionados con las tecnologías de la información y la comunicación). Se pueden negar las solicitudes de asistencia judicial recíproca si, por ejemplo, «están relacionadas con... delito(s) que la Parte requerida considere... delito(s) político(s) o delito(s) conectados con... delito(s) político(s)» (apartado 4 del artículo 25 del Convenio sobre Delitos Cibernéticos). También se pueden denegar las solicitudes de datos si la asistencia o la divulgación que se pide resulta en la violación de las obligaciones internacionales en asuntos de derechos humanos del Estado que responde (UNODC, 2013, pág. 204) (consulte Delitos Cibernéticos Módulo 3: Marcos Jurídicos y Derechos Humanos).

Según informe del Ministerio de Relaciones exteriores y culto (2022) Costa Rica suscribió el Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido también como Convenio de Budapest, el 14 de junio de 2022 para acceder a asistencia

mutua de urgencia y combatir la ciberdelincuencia. Se trata de un instrumento fundamental que permite a los Estados acelerar los procesos de cooperación internacional entre sus autoridades y obtener la colaboración directa de los proveedores ubicados en otros Estados ante la proliferación de la ciberdelincuencia.

El Protocolo, que fue adoptado por el Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021, es considerado como un instrumento fundamental que permitirá a los Estados acelerar los procesos de cooperación internacional entre sus autoridades y obtener la colaboración directa de los proveedores ubicados en otros Estados ante la proliferación de la ciberdelincuencia y de la complejidad creciente de la obtención de pruebas electrónicas que pueden ser almacenadas en jurisdicciones extranjeras, múltiples, cambiantes o desconocidas, (2022, p. 2).

El uso de la tecnología

Resulta innegable que el uso de la tecnología es uno de los medios idóneos para combatir la ciberdelincuencia, en los ciberdelitos la falencia de las medidas de seguridad de los sistemas informáticos es lo que los ciberdelincuentes atribuyen gran cantidad de su éxito, claro está que no todos los delitos informáticos se ejecutan por esas debilidades, pero el uso adecuado de ella minimiza los delitos.

> En los últimos años, se han llevado adelante infinidad de avances tecnológicos preparados específicamente para evitar fraudes y robos de datos financieros. Herramientas inteligentes como la tecnología biométrica, son avances realmente poderosos, las cuales analizan interacciones de humanos y dispositivos, protegiendo a usuarios de ataques o robos de identidad, (World Compliance Association, 2019, párr. 4).

El uso de la tecnología para prevenir la estafa informática resulta una herramienta indispensable para combatir este tipo de delito, los factores de doble seguridad como lo son los TOKEN, claves dinámicas y recientemente el uso de la biometría para el acceso al sistema bancario, celulares, y otras muchas plataformas más han contribuido al aumento de la seguridad.

Sin embargo, si no existe una cultura digital de poco sirve la tecnología para proteger los datos y el patrimonio de las personas, y es que esto ocurre por una brecha tecnológica, las personas que se nacieron en la era donde no se utilizaba internet son las más propensas a ser estafadas,

Para hablar del uso de la tecnología en la prevención de la estafa informática, se requiere una cultura digital enfocada al riesgo de una estafa informática en todas sus modalidades, siendo estas en su mayoría llamadas telefónicas, páginas de internet, porque, aunque existen mecanismos de seguridad tecnológicos, el principal problema es el usuario que brinda los datos sensibles a los delincuentes mediante la ingeniería social.

Y es que el uso de la tecnología y de las redes sociales ha permitido a los delincuentes mejorar sus técnicas delictivas en contra de sus víctimas, en donde el uso de herramientas tecnológicas e inteligencia artificial, ha permitido mejorar la ingeniería social de los delincuentes, como por ejemplo que los mensajes parezcan más reales y con eso cada vez más difícil de identificar las fuentes de la estafa por parte de las víctimas, de igual manera la obtención de datos personales de las víctimas, ya sea por instrumentos públicos como el registro civil, el registro nacional, que permiten verificar si las víctimas tienen propiedades familia, en la ingeniería social esos datos son utilizados para entablar una relación de confianza por parte del delincuente a su víctima.

Existen consejos de ciberseguridad que pueden utilizar las personas usuarias de la tecnología, y más aun las que no están tan relacionas con ella, puesto esta falta de interacción no permite dimensionar a la víctima del delito.

1. Desarrollar la malicia y la alerta digital para no caer en engaños.
2. Nunca atender una llamada telefónica cuando le dicen que procede de un banco. Cuelgue y llame usted al banco.
3. No brindar datos personales a desconocidos.
4. Evitar conectarse a una red desconocida. Y si lo hace, se recomienda tener en el teléfono o en la computadora un software antivirus y anti malware que le permita crear una red privada virtual (VPN).
5. No abrir correos de usuarios desconocidos y revisar la procedencia del mensaje.
6. Verificar la seguridad de los sitios web.
7. No compartir contraseñas.
8. Verificar la identidad de la persona con quien se está hablando.
9. Mantener el equipo informático actualizado.
10. Tener doble autenticación en las cuentas personales.

11. Conectarse desde la casa por medio de una VPN.
12. No apresurarse a darle clic a los enlaces. Tener precaución y revisar primero el enlace. Se debe copiar a mano para validar el mensaje.
13. Capacitarse para entender cómo funciona la tecnología, por ejemplo, un teléfono celular o una computadora y sobre cuáles medidas de seguridad debo tomar (UCR, 2023, párr. 48).

La formación de los profesionales

La formación de una policía especializada en el ciber crimen, representa una garantía para el estado en la lucha contra este tipo de delitos, siendo el caso de Costa Rica con una sección especializada de cibercrimen, donde son expertos en la materia informática junto con una formación de investigadores, el talento humano es la principal herramienta en contra del delincuente que se oculta detrás de la red de internet, los agentes de policía judicial especializados en cibercrimen, junto con equipos que le permite realizar una labor eficiente y eficaz, Brindarán una adecuada investigación dentro de los parámetros que la tecnología les permita y la astucia del delincuente.

> Los servicios policiales deben mantenerse actualizados en cuanto a los desarrollos tecnológicos y tener las habilidades y los conocimientos especializados necesarios para abordar una delincuencia digital en constante evolución a nivel nacional, regional e internacional, (Interpol, 2024, párr. 1).

Conviene hacer referencia del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) el cual publica en la Estrategia Nacional de Ciberseguridad 2023-2027 lo siguiente:

> El Gobierno de Costa Rica formuló su Estrategia Nacional de Ciberseguridad 2017-2021 permitiendo crear una institucionalidad que ha adelantado sus funciones y actividades en cabeza del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR). Si bien esta estrategia también ha permitido un avance significativo en asuntos de cooperación, de educación y de socialización frente al uso seguro de las Tecnologías de la Información y

> las Comunicaciones (TIC), es importante reforzar los esfuerzos para cerrar brechas en capacidades de ciberseguridad con el fin de que las múltiples partes interesadas aprovechen las oportunidades actuales y futuras que ofrece la Cuarta Revolución Industrial. (2023-2027, p. 2)

Para lograrlo se han formulado los siguientes objetivos:

Garantizar las condiciones para contar con un ecosistema nacional de ciberseguridad, seguro, resiliente e inclusivo que proteja de manera efectiva las infraestructuras críticas nacionales, los sectores público y privado y la ciudadanía de las ciber amenazas.

La Estrategia Nacional de Ciberseguridad 2023-2027 establece acciones que se dedican a todos los sectores de la economía y la sociedad, desde las instituciones de la administración pública central hasta los líderes de toda la industria y la ciudadanía, con el fin de alcanzar objetivos estratégicos y el objetivo general. La estrategia busca aumentar la ciberseguridad en todos los niveles para el beneficio colectivo y será la base a partir de la cual participará Costa Rica a nivel internacional para promover un ciberespacio más seguro. (MICITT, 2003 (pp. 18-25)

1. Reforzar la gobernanza de ciberseguridad
2. Adecuar el marco jurídico cibernético, para ello, Costa Rica desarrollará legislación y regulación cibernética junto con un marco normativo técnico para la ciberseguridad. Este pilar asegura la existencia de marcos legales y regulatorios robustos para promover la gestión integral de riesgos de ciberseguridad y hacer frente a las ciber amenazas.
3. Fortalecer la protección de infraestructuras y la ciber resiliencia nacional, Costa Rica establecerá un marco de gestión integral de riesgos de ciberseguridad que permita la detección, el reporte, el análisis y la respuesta oportuna a incidentes de ciberseguridad. Este pilar se enfoca en desarrollar capacidades para la respuesta a incidentes de ciberseguridad, así como la coordinación y la comunicación efectiva entre las partes interesadas durante las crisis cibernéticas.
4. Reforzar las capacidades del ecosistema de ciberseguridad, Costa Rica desarrollará una fuerza laboral capacitada en ciberseguridad a través de programas de educación, capacitación y formación, promoverá la conciencia de ciberseguridad entre el público y fomentará una cultura de comportamiento en línea responsable y seguro.

5. Cooperar en el entorno digital, Costa Rica impulsará la cooperación nacional e internacional, la colaboración y el intercambio de información sobre cuestiones de ciberseguridad. Este pilar enfatiza la participación en iniciativas, alianzas y foros internacionales para abordar las amenazas cibernéticas transfronterizas y promover normas de seguridad cibernética. (MICITT, 2023 (pp.18-25)

Retos en la individualización de la persona autora del delito de estafa informática.

De acuerdo con la (World Economic Fórum, 2022), la población más vulnerable a los ataques de ciberseguridad es la que recientemente se está conectando por vez primera a internet. Alrededor del 40% de la población mundial aún no está conectada y estas personas ya enfrentan desigualdades en seguridad digital.

Según (Larocca, 2022, p. 5). rtfgb cv

Ningún país o empresa puede afrontar la problemática de la ciberseguridad por sí solo y para encontrar la solución se necesitan estándares globales basados en la colaboración, siempre bajo una estricta revisión de todos los componentes de la cadena”

El programa malicioso apodado #WannaCry, por ejemplo, ya ha dejado más de 200.000 víctimas en todo el mundo, según una estimación de Europol, la agencia policial de Europa, y han empezado a surgir variantes del programa; por esta razón, los expertos sostienen que los efectos podrían aumentar a medida que más personas usen las computadoras atacadas.

Un crimen tan complejo, grande y global significa que, para que sea exitosa, la investigación requerirá de la colaboración cercana entre agencias internacionales —como el FBI, Scotland Yard y funcionarios de seguridad de China y Rusia— que usualmente son recelosas de compartir información las unas con las otras.

Dijo Brian Lord, ex subdirector de inteligencia y operaciones informáticas de Government Communications Headquarters la agencia de seguridad nacional británica: “Con el cibercrimen puedes operar de manera global sin tener que dejar tu casa”, “Encontrar a quien hizo esto va a ser muy difícil y requerirá de esa cooperación internacional que no se da de manera natural”.

El único acuerdo para la cooperación mundial en matera de crímenes informáticos es la Convención de Budapest, a la que solo pertenecen, en su mayoría, democracias del hemisferio occidental, dijo Nigel Inkster, exasistente en jefe para el servicio de inteligencia británico MI6. Gobiernos como el ruso y el chino han rechazado sumarse a la convención porque es el equivalente digital de una persecución callejera: la fuerza policial que investiga el crimen informático puede acceder a las redes de otras jurisdicciones sin pedir permiso.

La dificultad de identificar al autor

La dificultad de la identificación del delincuente estafa informática, se centra en la facilidad que este tiene de poder ocultarse a través del internet, o de cualquier otro dispositivo tecnológico como por ejemplo el teléfono, esto porque los medios para realizar la estafa como lo son el:

1. Phishing: Es el método de estafa por excelencia de los ciberdelincuentes y consiste en el envío masivo de correos electrónicos fraudulentos, suplantando la identidad de instituciones estatales (Agencia Tributaria, Policía Nacional, Correos, etc.), entidades financieras o empresas, cuya finalidad es conseguir que las víctimas accedan al enlace que contiene el correo, donde se les solicitará sus datos personales, claves bancarias y números de cuenta. Por otro lado, también puede consistir en la creación de sitios web falsos, donde igualmente se suplanta la identidad de ciertas entidades o instituciones y consiguen que las personas accedan e introduzcan los datos de sus cuentas bancarias o tarjetas de crédito.
2. SMiShing: es una modalidad de phishing y consiste en el envío de SMS que llega a las víctimas indicando que se han dado de alta en un determinado servicio, en el que se le cobrará cierta cantidad diaria o mensual a menos que cancele su petición llamando al número de teléfono que se indica o accediendo a un sitio web concreto. Para la cancelación del servicio y su correspondiente reembolso piden a las víctimas los datos bancarios suficientes para poder llevar a cabo su objetivo fraudulento
3. Vishing: Es un delito informático que se deriva del phising, pero no ofrece un enlace (link) para que la víctima haga click en él, sino que le ofrece un número de teléfono al cual comunicarse. Su nombre proviene de la unión de dos palabras en inglés: voice (voz) y phising. Para llevar a cabo el vishing, los delincuentes hacen uso de sistemas de

> telefónica IP o voz automatizada. Se realizan llamadas aleatoriamente a algunos números, a la persona que contesta se le informa que su tarjeta de crédito o cuenta bancaria está siendo utilizada fraudulentamente y deberá llamar a un número específico de su entidad bancaria; o, también se le puede solicitar datos personales llamando a un número telefónico específico. (Raúl, 2022, párr. 15-18).

Como se nota fácilmente, los delincuentes que cometen estafa informática lo hacen a través de un dispositivo conectado a internet, por lo que resulta complicado determinar cuál es el dispositivo, dónde se encuentra, quién lo manipula, quién es el autor intelectual del delito, todo gracias a internet, que al ser una red mundial el delincuente se encuentra en cualquier parte del mundo.

Para el autor del delito de estafa informática, el internet es un medio idóneo para ocultar su identidad, puesto los controles sobre las direcciones IP son casi inexistentes por parte de los proveedores de internet, en donde una persona puede comprar una conexión a internet y cualquier otra persona la puede utilizar, sin que la compra de la dirección IP se pueda configurar como un delito, pero si un medio que utiliza el delincuente de la estafa, para la materialización del delito es necesario el retiro del dinero, para lo cual se reclutan personas o se compran cuentas bancarias para eso, pudiendo ser el dueño de la cuenta un coautor del delito o simplemente una persona que facilita sus datos bancarios ante una solicitud de ayuda o un favor.

Las direcciones IP son fácilmente manipulables, siendo que pueden enmascarar la ubicación física de la misma, como se detalla:

1. Una VPN encripta sus datos y redirige su tráfico en línea hacia un servidor VPN dedicado antes de que se conecte al área pública de Internet. Al conectarse a un sitio web, el usuario se presenta como si proviniera de la VPN, de manera que su dirección IP auténtica se enmascara y el sitio web solo tiene acceso a la dirección IP de la VPN.
2. AVG Secure VPN tiene servidores en montones de países diferentes entre los que elegir, por lo que puede optar por aparentar ser de casi cualquier lugar. Esto es útil si viaja y quiere tener el mismo acceso a los servicios de streaming que utiliza en su país de origen. Proteja sus datos personales, no pierda el hilo de sus programas favoritos y mantenga la privacidad de su actividad en línea con AVG Secure VPN. (AGV, 2024, p. 3).

Las direcciones IP no se pueden considerar una fuente confiable para la investigación de la ubicación, o autor intelectual de los delincuentes de estafa informática, puesto la misma permite ocultarse a través de otras plataformas de internet encargadas de manipular la ubicación original.

Existe un factor que es determinante para las direcciones IP utilizadas por los delincuentes, y es que los mismos conocen el riesgo de utilizar una dirección de internet a su nombre y cometer un delito, por lo que esto podría asemejarse a robar un banco con la cara descubierta depositar el dinero en su cuenta y retirarlo, de esta forma sería muy fácil identificar al delincuente, los mismos se apareja con el delincuente que no previera utilizar direcciones de internet de terceras personas, de utilizar dispositivos y borrar la información que utilizó para cometer el delito etcétera, siendo todo eso muy fácil de realizar por parte del ciber delincuente, todo esto resulta en una dificultad para la identificación del mismo por parte de la autoridad judicial.

En el caso de las llamadas telefónicas o Vishing, ocurre algo similar que con las direcciones IP, los delincuentes enmascaran los números de teléfono donde realizan las llamadas cambiándolos por números conocidos de las entidades bancarias.

> Los estafadores utilizan diversas técnicas para que sus llamadas parezcan auténticas. Esto incluye el "spoofing" de números, que engaña al identificador de llamadas para mostrar un número similar o idéntico al de un banco o entidad de gobierno real. También suelen tener acceso a información personal parcial de las víctimas, como nombres o direcciones. Utilizan lenguaje y jerga bancaria, afirmando una emergencia o problema inmediato con la cuenta de la víctima para crear sentido de urgencia. En algunos casos, recurren a tácticas de intimidación o amenazas. Ofrecen soluciones rápidas, como proporcionar información personal o financiera para resolver un supuesto problema. (Banco Nacional, 2020, párr. 4).

Los delincuentes utilizan plataformas que permiten el enmascaramiento de números telefónicos similares a los de las entidades bancarias, esto es una herramienta tecnológica que el delincuente utiliza para su beneficio y perjuicio del usuario, puesto crea una falsa confianza de parte de la víctima que junto con técnicas de ingeniería social permiten que la víctima facilite información sensible como, usuario, claves de acceso, información de doble factor de seguridad como son los token, mientras el delincuente converse con la víctima esto mientras una tercera persona o él mismo ingresa los de acceso y realiza la transa hacia un fraudulenta a otra cuenta bancaria.

El delincuente que se oculta detrás de una llamada telefónica garantiza la seguridad de su identificación, puesto que la identificación de la voz del delincuente conlleva que este tenga que estar presente y anuente a someterse a una grabación para una comparación de la voz, esto en el caso de que la voz en el momento de la llamada sea grabada, lo cual la configuración de esos 2 elementos resulta casi imposible, en primer lugar, porque no se puede terminar quién es la persona que realiza la llamada.

La Dra. María Concepción Rayón Ballesteros y José Antonio Gómez Hernández en su investigación titulada "Cibercrimen: particularidades en su investigación y enjuiciamiento" (2014) hacen un recorrido general sobre el Cibercrimen, desde la perspectiva de la investigación y persecución junto con sus principales especialidades.

Uno de los aspectos de su investigación que interesan para el presente estudio es la ciberdelincuencia y las dificultades de su persecución. Al respecto refieren que:

> El desarrollo de Internet y de las nuevas tecnologías asociadas a la red relacionadas con la información y las comunicaciones hacen del ciberespacio un nuevo lugar para la perpetración de distintos ataques a bienes jurídicos tan importantes como la intimidad, el honor, la propiedad, la libertad sexual y hasta la integridad física y la vida. Aunque la mayoría de las conductas no son, en esencia, algo nuevo en sí mismas la extraordinaria particularidad del medio con el que se cometen, o sobre el que actúan, confiere a estas conductas una especial configuración que obliga a romper los esquemas clásicos para su investigación y enjuiciamiento. (p. 211).

Luego agregan que:

> Afortunadamente el Derecho Penal y el Derecho Procesal Penal han evolucionado para enfrentarse a ese nuevo cauce de ejecución delictiva que se desarrolla en un ámbito virtual y tecnológico, diferente al modelo tradicional de criminalidad física, individual e interpersonal, ya que cuestiona los axiomas vigentes. (p.211)

Consideran, por tanto, que es evidente que para hacer frente a esta forma de delincuencia se precisa realizar un enfoque supranacional, con unidades policiales de investigación especializadas y dotadas de los medios técnicos necesarios para la efectividad de su trabajo e, igualmente, se hace preciso un enjuiciamiento rápido y especializado de este tipo de conductas.

Como se ha señalado en el apartado correspondiente el Convenio sobre Ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001, y suscrito por el gobierno costarricense supone la respuesta a la necesidad de tener medios eficaces de cooperación internacional para la lucha contra la cibercriminalidad.

Luego agregan lo siguiente:

> Ciertamente la realidad delictiva siempre va por delante de la regulación legal y la correspondiente sanción punitiva de las conductas reprobables, pero, en estos casos en los que intervienen las nuevas tecnologías, muchísimo más dada la rapidez del desarrollo tecnológico, la facilidad del intercambio de la información, la comunicación inmediata entre lugares lejanos, la fugacidad de las acciones y la facilidad para conseguir su anonimato, la dificultad para identificar las huellas digitales, la fácil alteración de los rastros de la comisión de unos hechos, dificultad en la detección y la persecución de las conductas dañosas, el carácter transnacional de estas conductas delictivas junto con su insuficiente regulación legal y la escasa conciencia de los usuarios sobre la necesidad de mantener unas mínimas medidas preventivas de seguridad. (2014, p.214).

Explican los autores que, en este sentido, a efectos procesales, hay que matizar que la conducta delictiva puede tener su origen en uno o varios países y los resultados producirse en otro u otros, incluso puede resultar difícil determinar dónde se ha cometido la acción o por parte de quién. Obviamente esto afecta a la competencia jurisdiccional, a la ley penal aplicable y al procedimiento que se tramitará para su investigación y enjuiciamiento, ya que la regla general tradicional se refiere al lugar de comisión del delito (principio de territorialidad) contenido en la Ley Orgánica del Poder Judicial. De tal manera que el caso se complica cuando el hecho delictivo se pudo haber llevado a cabo en un país con una legislación incompleta o permisiva con respecto a conductas delictivas cometidas a través de las TIC, o que no poseen medios de detección y persecución ilimitados o que no han ratificado ningún tratado de extradición, lo cual dificulta aún mucho más la investigación y enjuiciamiento de estas conductas.

Un hecho que se debe destacar es que, en Costa Rica, en un mundo tan técnico y avanzado con las nuevas comunicaciones se hace necesario recurrir a expertos que asesoren en el modo de desarrollar la investigación por lo que los costes y el tiempo se incrementan considerablemente.

A lo anterior se agrega, como se ha venido tratando a lo largo de este estudio es la extraterritorialidad, que permite que se cometa el delito en un lugar y se produzcan los resultados en otro lugar distinto o que se cometan simultáneamente en diferentes lugares, a veces muy distantes, lo que dificulta también la investigación y la actuación de las autoridades policiales y judiciales. Lo cierto es que los datos de tráfico no siempre se localizan fácilmente.

Problemas de Persecución, la ciberdelincuencia y sus efectos son difícilmente descubiertas o perseguidas ya que los sujetos activos actúan sigilosamente, y poseen herramientas capaces de borrar todo rastro de intrusión o la consumación del delito, existen, según (Acurio, s.f, p. 57) dos problemas principales que a continuación se exponen:

Por lo dicho anteriormente se puede constatar en un primer momento que es difícil la persecución de estos delitos y su enjuiciamiento, ya que existe la posibilidad de preparar y cometer acciones delictivas informáticas en perjuicio de terceros en tiempo y espacio lejanos.

La importancia de los datos de tráfico, se ha venido reiterando la dificultad que ofrece la obtención de los datos del tráfico. Según lo exponen Rayón Ballesteros y Gómez Hernández (218, p. 215).

> Los datos de tráfico no siempre se localizan fácilmente. Generalmente se almacenan por los sistemas y aplicaciones informáticas y su conservación y el tiempo de ésta es configurable por el usuario que maneja el sistema. Para conseguir dichos datos tendremos que conocer el número IP, en el momento de conectarse a Internet, el momento concreto de acceso para la comisión del hecho dañoso, así como identificar el ordenador, su ubicación, el abonado de la línea telefónica o el contrato de acceso.

Al respecto los autores referidos consideran que, como regla general, realizando la investigación sobre los datos de tráfico, se podrá llegar a ubicar el equipo y a identificar al abonado, que no al usuario, pues puede ser otra persona diferente, por lo cual se hace necesario realizar la clásica vigilancia policial apoyada en los procedimientos comunes como vigilancia ordinaria, intervenciones telefónicas, rastreo de IP, etc.

En este sentido hay que destacar que los proveedores de servicio de Internet prestan una información determinante para la investigación, ya que los técnicos policiales necesitan básicamente los siguientes datos:

1. La dirección IP asignada al sospechoso por el proveedor y los datos contractuales (nombre y dirección) junto con la hora, fecha y duración de la comunicación, la concreta transacción o intercambio realizado.
2. La localización geográfica desde la que se conecta el sospechoso con el proveedor.
3. Las cuentas corrientes asociadas al pago de los servicios.
4. El número de teléfono de origen y destino de las comunicaciones realizadas por el sospechoso.
5. La concreta transacción o intercambio ilícito.
6. La copia de los ficheros de que disponga el sospechoso en su espacio web,
7. Las llamadas perdidas con determinación de su hora, duración y frecuencia.
8. El tipo de servicio telefónico empleado por el sospechoso.
9. El identificador del equipo en los teléfonos móviles.
10. Los datos de fecha y momento de activación de la tarjeta prepago de móviles, etc. (Rayón Ballesteros y Gómez Hernández (218, p. 215).

A partir de los datos obtenidos puede llegarse a determinar el lugar de comisión de los hechos, la máquina de origen, los autores de la conducta y el tipo de conducta punible que se ha perpetrado.

Según Rayón Ballesteros y Gómez Hernández (2018, p. 215), las medidas de investigación más eficaces para perseguir las conductas relacionadas con los TIC son:

1. La coordinación de entradas y registros en diferentes partidos judiciales a través de la vía del auxilio judicial.
2. La infiltración de agente encubierto en la red de la organización criminal.
3. La interceptación de las comunicaciones para descubrir sus componentes.
4. El método de actuación, y el destino final de los ingresos ilícitamente obtenidos.
5. La utilización de aparatos de escucha y filmación de actividades.
6. Las informaciones provenientes de delatores y confidentes.
7. La incautación de equipos.
8. La recuperación de logs, mensajes o backups.
9. El volcado de datos de dispositivos en los que se almacena la información.
10. Y en general la recogida y conservación de los efectos relacionados con el ilícito.

11. (Ballesteros y Hernández, 2018, 234).

En general, según criterio de los expertos hoy en día, como consecuencia del avance de las nuevas tecnologías, existen también herramientas eficaces de ciber-rastreo o monitorización consistentes en el uso de programas informáticos de *software* para la detección de rastros delictivos en la red y ofrecen buenos resultados.

La dificultad de probar el engaño

Según (Acurio, s.f, p. 59) en su estudio “Delitos Informáticos: Generalidades.

> 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 envión de correo no deseado o SPAM, en el cual se puede usar a 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.

El sujeto activo del delito puede fácilmente ocultarse a través del internet, esto utilizando direcciones IP, números de teléfono de otras personas, a través de la entidad de otra persona que pudo ser robada con anterioridad, estos son factores que dificultan probar quién fue la persona que se encargó del engaño en la fase del delito para con la víctima.

La evolución de los medios informáticos

La evolución de los delitos va de la mano junto con la evolución del internet, fue este caso de los medios tecnológicos que son creados para la facilidad de las labores cotidianas de la vida, lo cual aprovechan los delincuentes para beneficio suyo en su labor delictiva, y es que la evolución de los delitos los comunes, como la estafa, en dónde el engaño se hace en presencia de la persona

víctima para sustraer sus bienes, Con la tecnología pasamos a un nuevo delito que es la estafa informática, la cual se vale de dispositivos electrónicos para poder cometer el hecho delictivo por parte de los delincuentes.

La esencia del delito se mantiene, la cual es la sustracción del bien y por ende el menoscabo del patrimonio de la víctima, esto con el fin de aumentar el patrimonio de la persona delincuente, lo que ha evolucionado es el medio de cometer el delito valiéndose de la tecnología, como son programas de computadoras o llamadas telefónicas.

Y es que, si analizamos los tipos penales del Código Penal de estafa y de estafa informática, lograremos identificar la similitud del delito:

> Artículo 216, Estafa. Quien induciendo a error a otra persona o manteniéndola en él, por medio de la simulación de hechos falsos o por medio de la deformación o el ocultamiento de hechos verdaderos, utilizándolos para obtener un beneficio patrimonial antijurídico para sí o para un tercero, lesione el patrimonio ajeno, será sancionado en la siguiente forma:
>
> Artículo 217 bis. Estafa informática. 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.

Como se puede observar en el artículo 216, el delito se configura cuando se induce a error a otra persona o manteniéndolo en él, siendo esto en el delito estafa informática del 2017 bis lo denominado ingeniería social, en donde se utiliza esta técnica de engaño para manipular o influir en el ingreso de los sistemas bancarios de las víctimas, por lo que les delito de estafa informática es una evolución del delito de estafa que se da gracias al uso del internet y dispositivos electrónicos.

El rápido crecimiento de Internet también ha generado dilemas sociales, incluidas actividades ilegales o malintencionadas, y continuas discriminaciones digitales basadas en

diferencias de ingresos, procedencia, edad, sexo y educación. Estos problemas siguen requiriendo soluciones creativas por parte de científicos, legisladores y ciudadanos.

Juan Manuel Torres en su obra Evolución de los medios digitales, cómo se han transformado nuestra comunicación (2023) señala que:

> La evolución de los medios digitales ha cambiado la forma en que nos comunicamos y nos relacionamos con los demás de una manera significativa, desde los primeros chats y foros de los 90s, hasta los avances en la tecnología multimedia y la creciente influencia de las redes sociales y la publicidad en línea, los medios digitales han transformado la forma en que las empresas, las organizaciones y las personas interactúan y se comunican en línea, (p. 50).

Para que el delito de estafa surja es indispensable la interacción social, en un principio esta era a través de las palabras que se daban cara a cara, sin embargo, con la aparición del teléfono, la radio o la televisión, esta brecha de comunicación entre personas fue disminuyendo en distancias, hoy por lo que la identificación del delincuente se volvería más compleja.

Las primeras estafas con dispositivos se realizan por medio del teléfono, sin embargo, la tecnología en un principio no permitía enmascarar los números por lo que la identificación del delincuente podría ser más fácil, Con el uso de las computadoras conectadas a internet el anonimato del delincuente surte un auge, razón por la cual el internet se volvió un medio idóneo para cometer delitos de estafa.

La globalización de la ciberdelincuencia

Con la creación del internet se han disminuido las distancias para la interacción humana, por tal razón es entendible que se facilite la comunicación entre las personas, esta comunicación puede ser para efectos sociales, familiares o de negocios, este concepto se debe entender como globalización.

> Categoría social, política y económica que refiere a la uniformidad de costumbres y gustos a nivel mundial. || Interconexión mundial en todos los campos del quehacer humano. || En

> economía, proceso mundial en que los fenómenos mercantiles están determinados por las actividades financieras internacionales más que por una acción reguladora de los gobiernos nacionales, (Diccionario Poder Judicial, 2020).

Y es que la uniformidad que se da a través del internet permite un ambiente idóneo para los ciber delincuentes, los cuales utilizan la herramienta del internet junto con dispositivos tecnológicos para cometer los delitos, es por esto que dificulta aún más la individualización del autor de la estafa informática, porque puede estar en cualquier lugar del mundo y el internet burla esa brecha de distancia y fronteras entre los países que es ideal para cometer delitos por parte de los delincuentes.

Como ya se ha abarcado en este trabajo, la estafa informática representa el menoscabo del patrimonio de la víctima, pero es que además existe un mal aparejado a este, el cual es la pérdida de confianza del entorno digital, creando en las víctimas desconfianza del sistema bancario por la falta de responsabilidad ante la pérdida de su patrimonio, sin embargo, el factor real de la estafa informática se compone de la falta de malicia de la víctima ante la ingeniería social de los delincuentes, sin embargo el sistema de seguridad bancario debe brindar una protección extra ante esta modalidad de estafa informática, para la cual el uso de la tecnología ya es una aliada, pero la misma requiere la participación de la posible víctima.

> La realidad es que, "la materialización de ciberincidentes es una constante de la rutina diaria y cotidianeidad de gobiernos, empresas o individuos" de manera que el cibercrimen se ha convertido en un fenómeno mundial que afecta a todos los Estados, no tiene fronteras y la cantidad de posibles víctimas sigue aumentando con el crecimiento de la digitalización, toda vez que más ciudadanos, empresas, servicios públicos y dispositivos se encuentran conectados a Internet. Es por esto que se han comenzado a dar discusiones sobre la soberanía, las estrategias, la responsabilidad y los intereses de los Estados para adaptarse a los "ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) de gobiernos, administraciones públicas y empresas con alto valor estratégico" (UCR, 2023, párr. 7).

Los ciber delitos al no tener fronteras, aumenta exponencialmente el número de víctimas que sufren este tipo de ataque, de la cual tanto ciudadanos, empresas, instituciones del estado son víctimas de esta modalidad virtual, Y es que a nivel mundial la globalización permite la interacción

social a través de la comunicación digital, Para lo cual el mundo se ha preparado, como por ejemplo el convenio de Budapest o el convenio de NASSAU, donde la colaboración entre estados es fundamental contra la lucha de la ciberdelincuencia, permitiendo con ello aparejar la brecha de no fronteras en el internet, una colaboración activa entre estados miembros para la detención de ciber delincuentes, obtención de pruebas, custodia de las mismas, enjuiciamientos en el país de origen del delincuente, son parte de las medidas tomadas por el fenómeno de la globalización.

El Internet y la globalización han dado origen a un elemento que hoy en día se conoce como las redes sociales virtuales, el cual nos permite hacer contacto con personas que no están cerca de nosotros y no solo con una persona sino con varias, lo que facilita la interacción simultánea en el espacio virtual. De acuerdo con Merejo (2015, p. 1) la globalización tecnológica es la integración de los avances y herramientas técnicas alrededor del mundo, gracias al intercambio de conocimientos o actividades entre diferentes países que generan ventajas y beneficios a las personas en varios ámbitos.

La Nación publica en su artículo “La globalización del delito y la ciberdelincuencia” el 30 de abril 2017, que no solo beneficios han traído las tecnologías, también nuevas conductas delictivas. Y anota:

> La globalización moderna es más que un fenómeno exclusivamente económico, incluye aspectos sociales, culturales, políticos y también delictivos. Procesos de globalización han existido a lo largo de la historia de la humanidad, pero a la actual la identifican las tecnologías de la información y comunicación; no en vano se afirma que vivimos en la era digital, la era de Internet y de las redes informáticas. Nos encontramos ante una verdadera revolución tecnológica. Grandes han sido sus beneficios como profundos los cambios suscitados en la sociedad en un tiempo relativamente corto. La forma de trabajar, estudiar, relacionarnos con otros, hacer negocios y prácticamente todo en nuestra vida cotidiana está vinculado con las tecnologías de la información y la comunicación.

Considera el artículo que no solo beneficios han traído estas tecnologías, también grandes desafíos y nuevos problemas, entre ellos, nuevas conductas delictivas lo que ha permitido globalizar el crimen y ofrecido, concluye el artículo señalando que el desafío que se presenta ante la nueva delincuencia es mantener el equilibrio de un Estado de derecho sin sacrificar nuestras

garantías y libertades, y lograr una efectiva persecución y castigo de estas conductas con verdaderas garantías de protección, especialmente para las víctimas.

La necesidad de una cooperación internacional

La cooperación internacional, se sustenta de los tratados o convenios que los países suscriben entre sí, como por ejemplo el convenio de Budapest, el convenio de Nassau, estos convenios permiten una homogenización de los procesos judiciales penales en los casos de delincuencia internacional, en donde el delincuente se encuentra en un país ajeno a donde se comete el delito, siendo un Claro ejemplo de ello los ciber delitos, en los que se incluye la estafa informática, estos convenios contemplan el marco jurídico de los países, el cual debe ser sistematizado para que puedan funcionar y con garantía de derechos humanos.

Los convenios resulten convenientes para los estados, se necesita algo muy importante como lo es la doble incriminación, lo cual es que el delito cometido en el país afectado también sea delito en el país requirente de la colaboración, como lo establece el Convenio de Budapest, 2001, art. 25 inc. 5.

> Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia, constituya un delito en virtud de su derecho interno con independencia que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente.

La doble incriminación es necesaria para realizar las labores de investigación, puesto estas requieren según la legislación del país autorización de un juez, siendo el caso de Costa Rica, bajo el principio de debido proceso, legalidad de la prueba, prueba espuria, cadena de custodia, entre otros, ser recabados con las garantías que indica la convención interamericana de derechos humanos sobre el principio de inocencia.

También existen excepciones para el requisito de la doble incriminación, como es la conservación rápida de datos informáticos almacenados por medio de un sistema informático, esto cuando la parte requirente tenga la intención de presentar una solicitud de asistencia mutua para el

registro o un acceso similar, Esto porque se trata de una colaboración que se brinda de un país a otro, como lo establece el Convenio de Budapest, 2001, art. 29 inc. 3.

> Tras recibir la solicitud de otra Parte, la Parte requerida tomar· las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación.

Cuando la solicitud incluya actividades propias de un delito sustantivo en el país requirente, este país podrá denegar la solicitud de ayuda si el delito no está tipificado como tal en su legislación, por lo que la doble incriminación es un requisito fundamental para prestar esa colaboración, puesto de no hacerlo se estaría ante una violación al debido proceso en favor del imputado, siendo este por ejemplo allanamientos, prisión preventiva, etcétera, como lo establece el Convenio de Budapest, 2001, art. 29 inc. 4.

> Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.

Como parte de garantizar los derechos humanos de los delincuentes, existen tratados que resguardan estos derechos personalicemos como la vida humana, en donde el país requirente puede negar la extradición del delincuente si el país solicitante tiene penas de muerte, Cadena Perpetua, o infames, recordando siempre el resguardo de los derechos humanos de las personas, sin importar su condición de imputado, siendo el convenio interamericano sobre extradición de 1999, el que regula esta práctica en resguardo de las garantías personalísimas de la persona imputa, articulo 9.

> Los Estados Partes no deberán conceder la extradición cuando se trate de un delito sancionado en el Estado requirente con la pena de muerte, con la privación de libertad por vida o con penas infamantes, a menos que el Estado requerido obtuviera previamente del Estado requirente, las seguridades suficientes, dadas por la vía diplomática, que no

> impondrá ninguna de las citadas penas a la persona reclamada o que, si son impuestas, dichas penas no serán ejecutadas.

En la cooperación internacional es indispensable los convenios entre países, dichos convenios hacen una sistematización del de derecho internacional público con interés en el derecho penal, en donde se facilita la persecución de los delincuentes fuera de las fronteras del país donde se cometió el delito, pero siempre respetando los derechos humanos, es importante recalcar que el convenio de Budapest permite la investigación y recaudación de pruebas en los delitos cibernéticos, pero es junto a convenios de extradición donde se materializa la responsabilidad penal del imputado.

Como parte de los desafíos relacionados con la cooperación internacional, Ese el almacenamiento de datos, los cuales se almacena en servidores que se puede encontrar en cualquier parte del mundo, recordando que la cooperación internacional se enfoca principalmente en la recaudación de prueba y custodia en la misma, el país solicitante debe de conocer la ubicación donde se va a solicitar esos datos, para realizar la solicitud a la jurisdicción correspondiente.

> El problema con la informática en la nube es que es difícil saber dónde se almacenan los datos. Sin este conocimiento, no se puede identificar «la jurisdicción relevante a la que se debe dirigir la solicitud de cooperación para obtener la prueba, (UNODC, 2019, párr. 1).

Este problema de la obtención de datos en servidores ubicados físicamente en diferentes países se solventa con la ley nube, la cual le proporciona un marco legal a las agencias de investigación criminal, en dónde tras la solicitud las empresas prestadoras del servicio deben brindar todos los datos relacionados, esta ley aplica para Estados Unidos y empresas de tecnología estadounidense.

> En el 2018 Estados Unidos aprobó la “Ley Cloud” (CLOUD Act Clarifying Lawful Overseas Use of Data), la cual pondría fin al problema. Esta ley desarrolla dos puntos importantes:
>
> Concede a la fuerza del orden público de EE.UU., la posibilidad de emitir órdenes para que los datos almacenados en el extranjero sean proporcionados por parte de las empresas tecnológicas de EE. UU., es decir, a que se entreguen los datos almacenados en los servidores, ya sea que se almacenen en EE. UU. o en suelo extranjero.

> Permite acuerdos bilaterales con gobiernos extranjeros, para solicitar datos electrónicos de EE.UU., a cambio de acuerdos recíprocos. (García, 2020, párr. 5-7).

Como parte de los problemas de la cooperación internacional, es la falta de personal calificado para realizar las labores de investigación en el ambiente informático, en donde la falta de profesionales, recursos, instalaciones adecuadas, son uno de los principales obstáculos para que la cooperación internacional resulte exitosa en la lucha contra el cibercrimen.

> El déficit de capacidad nacional es el resultado de la falta de recursos humanos, financieros y técnicos (UNODC, 2013). Primero, muchos países no tienen la cantidad necesaria de personal cualificado para realizar las investigaciones de delitos cibernéticos, así como para procesar a los delincuentes cibernéticos y para manejar las solicitudes de cooperación internacional en asuntos de delitos cibernéticos. Segundo, los países no tienen los recursos financieros necesarios para reclutar, contratar y mantener al personal cualificado, y para brindar una capacitación actualizada y frecuente a los investigadores de delitos cibernéticos y a otros profesionales relacionados. Tercero, los países no tienen las instalaciones necesarias para analizar las pruebas digitales y carecen de los fondos necesarios para comprar el equipo y las herramientas para los análisis forenses digitales a fin de que puedan realizar adecuadamente las investigaciones de delitos cibernéticos, (UNODC, 2019, párr. 2).

La cooperación internacional es absolutamente imprescindible y se halla materializada en un conjunto de normas reguladoras de origen preferentemente convencional. El derecho interno tiende a facilitar la asistencia, de forma discrecional, atendiendo a principios de cortesía internacional o, más propiamente, de cooperación, utilizando con cierta frecuencia criterios de reciprocidad (Fernández y Sánchez, 2012).

Este espacio intangible al que se denomina ciberespacio, hay cuestiones que de no ser por la colaboración internacional entre los Estados y las que resultan de las interacciones entre los Estados y el sector privado, especialmente con los llamados proveedores de servicios, sería prácticamente imposible de resolver.

El Anonimato

El anonimato es el arma principal del ciber delincuente, ocultándose la identidad a través de la red de internet el autor de la estafa informática puede actuar o trabajar tranquilamente, de esta forma evadir responsabilidades, y con los sistemas informáticos actuales no necesariamente necesita una IP personal para cometer sus actos delictivos, al igual que con la llamada telefónica, existe una facilidad para obtener números telefónicos sin que el nombre de la propia persona sea el que registre el dueño de la línea, lo mismo ocurre con el internet, al igual existen programas que esconden o modifican la ubicación de las direcciones IP, siendo todas estas herramientas tecnológicas que facilitan la labor de la estafa informática a los ciber delincuentes, sumado a ello, utilizan terceras personas para realizar actos materiales del delito, como lo es la sustracción del dinero en las entidades bancarias o cajeros automáticos, realizando con ello la consumación del delito.

> 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 envío de correo no deseado o SPAM, en el cual se puede usar a 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 crakers 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 numero IP, (Acurio, s.f, p. 59).

El uso de la red de internet, para los ciberdelincuentes es un entorno en el cual se encuentran pocos riesgos de ser capturado y muchas oportunidades para cometer ciber delitos, es por esto la importancia de contar con medidas especiales de prevención por parte de los usuarios, entidades bancarias e instituciones gubernamentales y detección contra los ciber delincuentes, esto porque los ciber delitos no conocen de fronteras y la constante evolución de la tecnología los lleva siempre un paso adelante de la persecución penal.

Capitulo III: Marco Metodológico

Método e investigación

Conviene señalar la razón por la cual el enfoque metodológico que se empleará para tratar el reto de la individualización del autor o autores del delito de estafa informática en Costa Rica es el cualitativo. Al respecto se señala la Encyclopedia of Educacional Pysicology lo siguiente:

> La investigación desde la ruta cualitativa se enfoca en comprender los fenómenos, explorándolos desde la perspectiva de los participantes en su ambiente natural y en relación con el contexto. Se selecciona el enfoque cualitativo cuando el propósito es examinar la forma en que ciertos individuos perciben y experimentan fenómenos que los rodean, profundizando en sus puntos de vista, interpretaciones y significados, (Hernández, Fernández y Baptista, 2018, p. 390)

En relación con la cita anterior, Hernández, Fernández y Baptista (2018), complementan que "los estudios cualitativos utilizan la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación." (p.7).

Este trabajo se concibió como una investigación cualitativa de modalidad estudio de caso, de método inductivo. El estudio hace uso de un diseño de teoría fundamentada para el tratamiento de la información que se recolectó Hernández (2018). La categoría de análisis principal es determinar los retos de la individualización del autor o autores del delito de estafa informática.

Se deduce de la cita anterior que se cuenta con una variedad de técnicas y recursos para recolectar la información, lo cual difiere del enfoque cuantitativo en cuanto que no procura medir variables. Así, reforzado por (Hernández, Fernández y Baptista, 2018, p.390).

Para complementar la definición del enfoque cualitativo se hace referencia a Gutiérrez (1994) en Barrantes (2014, p. 91) quien señala que:

> Los enfoques cualitativos buscan llegar al conocimiento "desde dentro" (Stromkist,1989, en Barrantes,2000), por medio del entendimiento de intenciones... por lo tanto el enfoque cualitativo es más inductivo que deductivo. Por lo tanto, la investigación cualitativa postula

una concepción fenomenológica, inductiva, orientada al proceso. Este enfoque pone énfasis en la profundidad y sus análisis.

En el desarrollo del presente trabajo se analizarían los principales retos que se presentan para la individualización del autor o autores del delito de estafa informática. Estos retos se pueden agrupar en dos categorías: Los recursos técnicos y los recursos jurídicos.

Dentro de las conclusiones se sintetizarían los principales resultados del análisis y se harían algunas recomendaciones para mejorar la individualización del autor o autores del delito de estafa informática. Aquí se debe incluir las posibles soluciones para superar los retos identificados. Estas soluciones pueden ser de naturaleza legislativa, judicial o policial.

Técnicas de investigación

Entrevista a profundidad

Como parte de lo que es un estudio cualitativo, se realizaran las técnicas de investigación relacionadas a la entrevista a profundidad, la cual es fundamental para el desarrollo de los objetivos específicos y desarrollar el problema de investigación, este responde a los sujetos seleccionados bajo un criterio objetivo de su relación con el tema en su ámbito laboral.

La entrevista a profundidad consiste en recopilar la información formulando preguntas. A través de la comunicación interpersonal, el emisor obtiene respuestas verbales del receptor sobre un tema o problema en específico. Esta se podrá realizar de forma presencial, por teléfono o WhatsApp. (Escudero C.L y Cortez, L A, 2018).

Robles (2011) señala al respecto que:

> La entrevista en profundidad se basa en el seguimiento de un guion de entrevista, en él se plasman todos los tópicos que se desean abordar a lo largo de los encuentros, por lo que previo a la sesión se deben preparar los temas que se discutirán, con el fin de controlar los tiempos, distinguir los temas por importancia ...
>
> La entrevista en profundidad se basa en el seguimiento de un guion de entrevista, en él se plasman todos los tópicos que se desean abordar a lo largo de los encuentros, por lo que

> previo a la sesión se deben preparar los temas que se discutirán, con el fin de controlar los tiempos, distinguir los temas por importancia y evitar extravíos y dispersiones por parte del entrevistado, (p. 5)

Agrega Robles (2011) que el guion debe estructurase con base en la hipótesis y los objetivos de nuestra investigación, en él se incluirá una introducción donde el entrevistador dará a conocer el propósito de la entrevista, cómo estará estructurada y qué alcances se desean obtener. Es importante que los entrevistados tengan claro que toda la información que se obtenga se analizará con atención y cuidado, atendiendo en todo momento la confidencialidad de los datos. Asimismo, el guion contendrá todas las temáticas a estudiar y que deberán desarrollarse a lo largo de todas las sesiones.

La entrevista a profundidad será fundamental para el presente trabajo, la cual tiene por objetivo la recolección de información de primera mano con personas que hayan contado con la experiencia en delitos de estafa informática, para lo cual se realizó la siguiente selección de sujetos:

1. Un miembro del Poder Judicial que labore en la sección de cibercrimen
2. Dos Jueces de la materia penal
3. Un Fiscal con experiencia en dirigir la investigación sobre el delito de estafa informática
4. Un Defensor Público.

Análisis de jurisprudencia

Como parte de las herramientas del estudio cualitativo, se realizará el análisis de jurisprudencia relevante para el tema de investigación, el cual trata de evidenciar la problemática en la individualización de los autores en la estafa informática, así mismo los problemas para acreditar la coautoría del delito por parte del Tribunal de Juicio encargado del caso y con ello sentar la participación del coautor del delito.

Se tomará para el estudio del trabajo jurisprudencia de los años 2020 al 2023, de los tribunales de apelación de sentencia del país, siendo sujeto a análisis la siguiente:

1. Resolución N°01164-2023 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las nueve horas veinte minutos del seis de setiembre de dos mil veintitrés.
2. Resolución Nº 00256 – 2023 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las siete horas con cincuenta y cinco minutos del veinte de febrero de dos mil veintitrés.
3. Resolución Nº 01838 – 2022 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las nueve horas quince minutos, del veinte de diciembre de dos mil veintidós.
4. Resolución Nº 00950 – 2022 del Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón, de las once horas cuatro minutos del veintiuno de octubre de dos mil veintidós.
5. Resolución 00284-2022 del Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón
6. Resolución Nº 00851 – 2022 del Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón, de las once horas quince minutos del veintidós de setiembre de dos mil veintidós.
7. Resolución Nº 01862 – 2021 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las diez horas cinco minutos del dos de diciembre de dos mil veintiuno.
8. Resolución Nº 01398 – 2021 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las once horas treinta minutos del quince de setiembre de dos mil veintiuno.
9. Resolución Nº 00772 – 2020 del Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón, de las quince horas cincuenta y cinco minutos del veintiuno de agosto de dos mil veinte.
10. Resolución Nº 01145 – 2020 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las diez horas, del catorce de julio de dos mil veinte.

Capítulo IV. Análisis de Resultados

Como se señaló en el marco metodológico se realiza la entrevista a profundidad a un juez de tribunal, un juez de la etapa intermedia, el fiscal coordinador de la sección de ciber crimen, un fiscal auxiliar, una defensora publica, así como de diez jurisprudencias de los periodos 2018 a 2023.

Análisis de resultados

Experiencia

Sobre la experiencia en delitos informáticos, todos los funcionarios del Poder Judicial que colaboraron para la presente entrevista, poseen experiencia en delitos de estafa informática, con lo cual existe un dominio del tema sobre el tipo penal.

Experiencia de los jueces, el juez penal de la etapa de juicio, manifiesta que no posee una capacitación específica sobre el delito de estafa informática, sino que la experiencia se adquiere por los asuntos relacionados a las acusaciones, lo mismo ocurre con el juez penal de la etapa intermedia, donde no posee una capacitación específica sobre este tipo de delitos, pero sí por su experiencia en la posición del puesto y la gran cantidad de audiencias preliminares le han permitido tomar experiencia sobre el delito de estafa informática.

En cuanto a los fiscales, la experiencia del fiscal coordinador de la unidad de cibercrimen, se concreta específicamente en trabajar en la unidad especializada, de la cual posee cuatro años de trabajar en esta unidad, de estos año y cuatro meses como Jefatura, por lo que la cantidad de delitos cibernéticos le ha permitido tomar experiencia y capacitación, al pertenecer a una unidad especializada los únicos delitos que conoce son los relacionados a ciberdelincuencia, en el caso del fiscal auxiliar, este asevera que al pertenecer a una Fiscalía distrital atiende todo tipo de delitos, siendo uno de ellos el de la estafa informática por lo cual tiene experiencia en el tema.

En el caso de la defensora pública, ella no ha tenido una especialidad sobre delitos de estafa informática, sin embargo, al ser un servicio que la defensa pública ofrece de la defensa de imputados, sí posee experiencia en la defensa de personas relacionadas con estafa informática.

Con el dato brindado por las personas entrevistadas, se puede llegar a la conclusión que la experiencia obtenida en el delito de estafa informática se fundamenta principalmente en la práctica judicial propia de sus funciones, y no porque exista una capacitación de este tipo penal específico para funcionarios que laboran en la materia penal.

La incidencia de los delitos de estafa informática

El delito de estafa informática es un delito en aumento constante, en donde todos los entrevistados confirman el hecho de que este tipo de delito ha venido en aumento, tomando como referencia los años de laborar para el Poder Judicial, siendo el fiscal coordinador de la sección de ciber crímenes el que enumera más precisamente este dato, en donde indica que en el año 2018 ingresaron 3000 denuncias, mientras que para el año 2023 se cerró con más de 13000 denuncias de estafa informática, siendo un crecimiento mayor al 450% en un plazo de 5 años.

Como factor recabado en las entrevistas, se evidencia como razón de aumento de las estafas informáticas, la demografía, en donde cada día hay mayor cantidad de personas, las cuales son las víctimas de los delincuentes, y no solo en delitos de estafa informática, pero sí ha sido un factor determinante para el aumento de los casos, otro punto importante que ha sido referencia para este aumento fue la pandemia, en donde el confinamiento por parte del Poder Ejecutivo como control del virus, puso a los usuarios a un mayor contacto con la tecnología, siendo esto aprovechado por los delincuentes cibernéticos, además se debe tomar en cuenta como otro punto importante es el grupo etario, en dónde las personas adultas, o adultos mayores han sido la mayor cantidad de víctimas afectadas por los ciber delincuentes, esto por su condición de una relación con la tecnología en la edad adulta, siendo con ello la falta de cuidado y confianza a la hora de ser engañados por ingeniería social.

El medio para cometer el delito de estafa informática

El medio más utilizado para cometer estafa informática, Indudablemente ha sido la ingeniería social, a lo cual la mayoría de la jurisprudencia y todos los entrevistados llegan a coincidir, siendo a través de las llamadas telefónicas, la cual se complementa con una manipulación de sistemas informáticos, el delincuente a través de su astucia y facilidad de palabra, crea un

vínculo con la víctima, haciéndola creer que realmente se trata de personal de la entidad bancaria o institución pública, logrando con ello que la víctima facilite información importante como lo es, correo electrónico, usuario, contraseña y doble factor de seguridad, siendo con ello que el delincuente ingresa a la plataforma bancaria y hace el traslado fraudulento de los dineros de la víctima.

Es a través de la jurisprudencia y los entrevistados que se determina como medio principal para estafar la llamada telefónica y la manipulación de la página bancaria, siendo el Vishing la primera estrategia de estafa, para posteriormente y en el mismo acto realizar la manipulación de la página del Banco de la víctima, en este caso los entrevistados identifican como medio fraudulento la llamada telefónica, puesto la manipulación del sistema se realiza en la página oficial y la obtención de datos son facilitados por la víctima bajo el engaño, los entrevistados no identifican como principal medio el uso de Phishing o malware, sin embargo si lo mencionan como medios para estafar a las víctimas.

La participación de una o más personas delincuentes

Esta respuesta fue categórica por parte de la jurisprudencia y todos los entrevistados, en indicar que en los delitos de estafa informática participan diferentes autores, pudiendo identificar como mínimo: la persona que realiza la llamada telefónica, la persona que brinda los datos de la víctima, la persona que manipula el sistema informático bancario, la persona que recluta a los sujetos que facilitan la cuenta bancaria y los sujetos que retiran el dinero, por lo que estamos ante una coautoría.

En el caso del juez penal de la etapa de juicio, identifica la participación de un solo individuo en la estafa informática, donde, a través de páginas de compra y venta de artículos, el delincuente publica un artículo para la venta, siendo el caso que el comprador deposite el dinero y este no le entrega el artículo por ser una estafa, también una única jurisprudencia identifica un único autor, siendo el caso del delincuente que roba una tarjeta de débito y solicita a la víctima la clave, para posterior ir a retirar el dinero manipulando el cajero automático.

El fiscal coordinador de la sección de ciber crimen y el juez penal de la etapa intermedia manifiestan que en muchos casos la ciberdelincuencia se trata como delincuencia organizada, esto

por la participación de tres o más autores, con ello brindando más herramientas para la identificación de los ciber delincuentes como lo es la intervención telefónica.

Se logra llevara juicio a todos responsables del delito de estafa informática

Categóricamente la respuesta es no, todos los entrevistados coinciden en su respuesta, la cual es que no todos los autores del delito estafa informática son localizados y llevados al proceso penal, que si bien es cierto se logra determinar al que sería en primera línea el imputado que es la persona que retire el dinero o facilita la cuenta, lo cierto es que por ser un delito de varios autores no todos son llevados al proceso penal, así lo describen los jueces, fiscales y la defensora pública.

El mismo hallazgo arroja la jurisprudencia, en donde la única persona imputada es la dueña de la cuenta o quien retira el dinero, en donde no figuran más personas imputadas para el delito de estafa informática.

Sobre las pruebas en el proceso penal del delito de estafa informática

Estas en su mayoría se componen de prueba documental, siendo el levantamiento del secreto bancario y vídeos de seguridad como las pruebas que se recaban en primera instancia, el criterio de los jueces y es confirmado por los fiscales del ministerio público, es la falta de herramientas tecnológicas para la investigación del delito de estafa informática lo que imposibilita presentar más pruebas al proceso.

Otro aspecto importante con la recaudación de prueba, según indica el juez de la etapa de juicio, tiene que ver con la experiencia del fiscal a cargo de la investigación, donde él ha tenido que ordenar la devolución del expediente a la etapa de investigación para que se realicen otras diligencias pertinentes para la obtención de prueba.

También se debe tomar en cuenta la falta de colaboración de las entidades financieras por resguardar información relevante para la acreditación de los hechos, según lo indica el fiscal de la sección de cibercrimen.

La jurisprudencia también arroja que la prueba documental es la protagonista en los delitos de estafa informática, siendo que en un solo caso analizado se ofreciera prueba testimonial, pero esta radica en la manifestación de la agente del OIJ cuando la víctima le relato el suceso.

Sobre la colaboración de las personas imputadas para identificar los otros autores del delito

La colaboración que brindan las personas imputadas para lograr identificar a autores del delito de estafa informática es nula, según los resultados de la entrevista, manifiesta el juez de la etapa intermedia y el fiscal de la sección de cibercrimen del ministerio público, que los imputados se acogen a su derecho de abstención, resultando materialmente imposible poder obtener información, además como parte de la información que brindan coinciden ambos profesionales que solo manifiestan que no conocen a la persona que les prestaron la cuenta y que solo hicieron un favor a un desconocido, en el caso de la jurisprudencia ocurre lo mismo, los imputados manifiestan que no conocen a la persona, que solo hicieron un favor de prestar la cuenta para recibir la transferencia y retirar el dinero.

Las personas imputadas, si colaboran con la investigación pero para acogerse a algún tipo de beneficio, como lo es el criterio de oportunidad o la conciliación, según lo indica del fiscal del ministerio público, ante esto indica la defensora pública que si el ministerio público tratara a los imputados como testigos se podría lograr mayor información, a lo cual contradice el fiscal de la sección de cibercrimen, pues lo que se realiza es una acusación en coautoría esto es por la forma en que se realiza el delito y actúa la persona imputada.

Herramientas tecnológicas que podría ser útiles para la identificación del ciberdelincuente

Con la ayuda de la tecnología se podría realizar una investigación adecuada al tipo de delito de estafa informática, los representantes de la fiscalía manifiestan que es necesaria la inversión en tecnología, existen programas que permiten un rastreo de direcciones IP, desbloqueo de teléfonos

e inteligencia artificial, todos como el fin de hacer una comparación de datos y rastreo dentro de la web.

Los jueces por su parte manifiestan que es necesaria la inversión también en tecnología para la adecuada investigación por parte del ministerio público, sin embargo, el juez de la etapa intermedia manifiesta que con la intervención telefónica se podría realizar una investigación más profunda y con ello escalar dentro de la organización delictiva de la estafa informática hasta llegar a niveles más altos, recalca que con una reforma al artículo nueve de la ley de secuestro y registro en donde se incluya al delito de estafa informática se podría realizar investigaciones sin declaratoria de crimen organizado. Como otra medida el juez de la etapa de juicio indica que si se lograra asignar una dirección IP personal a cada sujeto el problema de la identificación del delincuente que utiliza medios tecnológicos podría facilitarse.

Recomendaciones generales para mejorar la identificación del ciberdelincuente

Como recomendaciones emitidas por el juez de la etapa intermedia, sería la especialización de la policía judicial y personal del ministerio público, así como la modificación del artículo 9 de la ley de secuestro y registro, integrando el delito de estafa informática como uno de los delitos a investigar con intervención telefónica.

Como parte de las recomendaciones el fiscal de la sección de cibercrimen y la defensora publica indica que parte de las soluciones sería el involucramiento del sector bancario, proveedores de internet y telefonía, al igual que los centros penales donde se ha identificado que se gesta la delincuencia cibernética propiamente la ingeniería social.

Asimismo, el fiscal auxiliar ve viable como una recomendación el mejorar la situación tecnológica que poseen en este momento, porque, aunque existen herramientas procesales como los criterios de oportunidad para que el delincuente colabore con la investigación, lo cierto es que no colabora, siendo que con herramientas tecnológicas pueden realizar mejores investigaciones para tratar de identificar al ciber delincuente.

Análisis de jurisprudencia

Como parte de las herramientas del estudio cualitativo, se realizará el análisis de jurisprudencia relevante para el tema de investigación, el cual trata de evidenciar la problemática en la individualización de los autores en la estafa informática, así mismo los problemas para acreditar la coautoría del delito por parte del Tribunal de Juicio encargado del caso y con ello sentar la participación del coautor del delito.

Se tomará para el estudio del trabajo jurisprudencia de los años 2020 al 2023, de los tribunales de apelación de sentencia del país, siendo sujeto a análisis la siguiente:

11. Resolución N°01164-2023 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las nueve horas veinte minutos del seis de setiembre de dos mil veintitrés.
12. Resolución Nº 00256 – 2023 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las siete horas con cincuenta y cinco minutos del veinte de febrero de dos mil veintitrés.
13. Resolución Nº 01838 – 2022 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las nueve horas quince minutos, del veinte de diciembre de dos mil veintidós.
14. Resolución Nº 00950 – 2022 del Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón, de las once horas cuatro minutos del veintiuno de octubre de dos mil veintidós.
15. Resolución 00284-2022 del Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón
16. Resolución Nº 00851 – 2022 del Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón, de las once horas quince minutos del veintidós de setiembre de dos mil veintidós.
17. Resolución Nº 01862 – 2021 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las diez horas cinco minutos del dos de diciembre de dos mil veintiuno.

18. Resolución Nº 01398 – 2021 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las once horas treinta minutos del quince de setiembre de dos mil veintiuno.
19. Resolución Nº 00772 – 2020 del Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón, de las quince horas cincuenta y cinco minutos del veintiuno de agosto de dos mil veinte.
20. Resolución Nº 01145 – 2020 del Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José, de las diez horas, del catorce de julio de dos mil veinte.

Análisis de Jurisprudencia

Jurisprudencia N° 1.

Delito: Estafa Informática

Resolución: 1164-2023

Despacho: Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José

Fecha: 06 de Setiembre del 2023 a las 09:20

Análisis:

1. Medio de cometer el delito: Ingeniería social; llamada telefónica indicando que el banco estaba pasando de cuenta cliente a cuenta IBAN, que necesitaba hacer unas pruebas y requerían la información de acceso a la cuenta.
2. Sujeto pasivo: Persona física
3. Se individualiza al sujeto activo del delito: No
4. Coautoría: Dos sujetos, no se demuestra que manipularan los sistemas informáticos para cometer el delito, el titular de la cuenta presta la cuenta para que depositen una incapacidad de su amiga y compañera de trabajo de varios años,
5. Pruebas: Documental
6. Monto defraudado: ¢ 620 000

7. Bancos intervinientes: Victima poseía el dinero en el Banco Nacional de CR, Banco de Costa Rica donde se deposita el dinero y es retirado ¢500 000 en cajero automático y ¢ 120 000 en compra de anillo en casa de empeño.
8. Otros: A- La pieza acusatoria; no indica que los imputados realizan la acción de manipulación en los sistemas informáticos del banco para extraer el dinero, B- tampoco señala que existiera un plan común entre los imputados y el sujeto activo que realizo la conducta típica, C- no habla de una distribución de funciones. D- Falta de investigación; del imputado que presto la cuenta para verificar el vínculo con la otra imputada, E- sobre la imputada que solicito el favor de utilizar la cuenta no hubo investigación sobre si alguien cercano a ella sufriera incapacidad, F- no se investigó si la llamada salió del Banco Nacional o alguna maniobra para simular el número.
9. Resultando de Tribunal Penal de San José, sentencia 42-2023 de las 15:47 del 1-01-2023: Absuelve por principio in dubio pro reo y por certeza a los dos imputados
10. Resultando Tribunal de Apelación de Sentencia: Se declara sin lugar el recurso de apelación interpuesto por el representante del Ministerio Público

Jurisprudencia N° 2.

Delito: Estafa informática

Resolución: 256-2023

Despacho: Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José

Fecha: 20 de febrero del 2023 a las 07:55

Análisis:

1. Medio de cometer el delito: Ingeniería social, presidenta de la sociedad recibe llamada de quien le compraría unos muebles, otro la llama y se hace pasar por funcionario del BCR y le solicita datos de acceso de su cuenta para poder hacerle el depósito del pago de los muebles, ingresan a la cuenta y transfieren el dinero y es retirado en ventanilla,
2. Sujeto pasivo: Persona jurídica (presidenta engañada)
3. Se individualiza al sujeto activo del delito: No

4. Coautoría: Si, No es posible; A- determinar quien fue la persona que engaño a la ofendida para proporcionar los datos de su cuenta, B- ni quien materialmente realizo la transferencia fraudulenta de dinero, C- el imputado participo de manera activa en tal delincuencia, tanto porque es beneficiario directo del dinero transferido a su cuenta, su cuenta se apertura 7 días antes, esa cuenta solo posee dos movimientos (depósito y retiro)
5. Pruebas: Documental
6. Monto defraudado: $ 4 002
7. Bancos intervinientes: Victima poseía el dinero en el Banco de CR, se deposita en cuenta del Banco Popular y lo retiran de ventanilla en Plaza Lincoln,
8. Otros: A- apelación planteada por la defensa, fundamentada por cuestionar la valoración de la prueba que realiza el Tribunal, B- el TAS dice "Toda esta maraña de acciones se tuvo por acreditada mediante una plataforma probatoria sólida y objetiva, como lo es la información bancaria que revela los movimientos dinerarios realizados, existencia de la cuenta del encausado y que ese fue el destino de los dólares sustraídos a la ofendida y el testimonio de ella, el cual se consideró veraz. "El acusado accedió a la petición de la persona de calidades desconocidas y le facilitó a este el número de su cuenta bancaria",
9. Resultando de Tribunal Penal del II Circuito Judicial de San José, sentencia 1227-2022 de las 22:06 del 01-12-2022: Autor responsable por el delito de estafa informática, pena de cinco años de prisión, sustituía por arresto domiciliario electrónico.
10. Resultando Tribunal de Apelación de Sentencia: Se declara sin lugar el recurso planteado por la defensa.

Jurisprudencia N° 3.

Delito: Estafa informática

Resolución: 1838-2022

Despacho: Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José

Fecha: 20-12-2022 a las 09:15

Análisis:

1. Medio de cometer el delito: Phishing, la victima ingreso a lo que creía era la página oficial del BCR, el sistema le solicito la clave, pero generaba errores, digito su clave dinámica. Posterior se percata que se realizaron dos transferencias a terceros desconocidos,
2. Sujeto pasivo: Persona jurídica
3. Se individualiza al sujeto activo del delito: No
4. Coautoría: Un imputado se apersona a retirar en el cajero automático,
5. Pruebas: Testigo de referencia una agente del OIJ, documental,
6. Monto defraudado: total $ 3991.85 ($ 1 996. 84 + $ 1 995.01)
7. Bancos intervinientes: Victima era cliente del BCR, Primera transferencia fraudulenta al Banco Nacional el 19-3-2013, segunda transferencia fraudulenta al Banco Popular 20-03-2013 que es la cuenta del imputado.
8. Otros: A- recurso planteado por la defensa, fundamentado en que no se evacuo la declaración del ofendido, B- sistema penal costarricense permite cualquier medio de prueba siempre que sea licito, el Tribunal le asignara el valor correspondiente, C- dirección IP de donde se realizó la transferencia fraudulenta se encuentra en San José y la victima reside en Playa Hermosa Zona Sur, D- cuenta del Banco Popular fue abierta un día antes del depósito fraudulento,
9. Resultando de Tribunal Penal I Circuito Judicial de San José de las 14:30 del 14-07-2022: autor responsable de un delito de ESTAFA INFORMÁTICA, cinco años de prisión, se revoca beneficio de ejecución de la pena por tres años por el delito de robo agravado, se unifican las penas a un total de ocho años.
10. Resultando Tribunal de Apelación de Sentencia: debiendo el sentenciado [Nombre 001] cumplir únicamente la pena de cinco años de prisión que se le impuso en el presente proceso, al encontrarlo culpable del delito de fraude informático en perjuicio de [Nombre 002].

Jurisprudencia N° 4.

Delito: Estafa informática

Resolución: 950-2022

Despacho: Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón

Fecha: 20 de febrero del 2023 a las 07:55

Análisis:

1. Medio de cometer el delito: Ingeniería social, autor del delito se hace pasar por representante de Hacienda, dando un link falso de la página del Ministerio de Hacienda, la victima brinda información sensible de su cuenta, posterior a ello se transfiere dinero de manera fraudulenta a cuenta del imputado.
2. Sujeto pasivo: persona física
3. Se individualiza al sujeto activo del delito: No
4. Coautoría: Si, no demostrada
5. Pruebas: Documental, aceptación de hechos por proceso especial abreviado.
6. Monto defraudado: ¢ 470 000
7. Bancos intervinientes: Cuenta de la víctima en Banco Nacional, cuenta del imputado Banco Nacional.
8. Otros: A- defensa publica apela falta de fundamentación intelectiva en cuanto a la participación del imputado en la comisión del delito, B- imputado facilita la cuenta a un tercero sin identificar para que este reciba unos dineros, C- se acordó un procedimiento especial abreviado.
9. Resultando de Tribunal de Juicio de Heredia de las 11:45 del 27-4-2022; autor responsable de un delito de Estafa informática, dos años de prisión,
10. Resultando Tribunal de Apelación de Sentencia: Se declara sin lugar el recurso de apelación de sentencia promovido por la defensa

Jurisprudencia N° 5.

Delito: Estafa informática

Resolución: 284-2022

Despacho: Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón

Fecha: 05 de abril del 2022 a las 13:20

Análisis:

1. Medio de cometer el delito: Ingeniería social, por llamada telefónica haciéndose pasar por Ministerio de Hacienda para actualizar datos por medio de representante del Banco Nacional,

2. Sujeto pasivo: Persona física

3. Se individualiza al sujeto activo del delito: No

4. Coautoría: Si

5. Pruebas: Documental, testimonial de agente de OIJ y ofendida.

6. Monto defraudado: ¢ 5 400 000

7. Bancos intervinientes: Cuenta de la víctima Banco Nacional, cuenta donde se deposita el dinero Banco Popular

8. Otros: A- recurso de apelación interpuesto por defensa publica por inconformidad con la fundamentación de la sentencia, en detrimento del principio in dubio pro reo, B- imputada se abstuvo de declarar, C- imputada alego que no se confronto su firma del Boucher para saber si es ella la que retira el dinero, D- imputada indica que fue contactada por un hombre para que le facilitara la cuenta y le depositaran un dinero.

9. Resultando de Tribunal de Juicio del Segundo Circuito Judicial de Alajuela, San Carlos, de las 13:25 del 29-4-2021, autora responsable de haber cometido el delito de Estafa Informático, condena a 2 años de prisión, Por cumplir con los requisitos legales se le concede el Beneficio de Ejecución Condicional de Pena, por un período de prueba de 3 años.

10. Resultando Tribunal de Apelación de Sentencia: Se declara sin lugar, el recurso de apelación presentado por el defensor de la imputada

Jurisprudencia N° 6.

Delito: Estafa informática

Resolución: 851-2022

Despacho: Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón

Fecha: 22 de Setiembre del 2022 a las 11:15

Análisis:

1. Medio de cometer el delito: Ingeniería social, llamada telefónica haciendo pasar por cliente de la empresa y solicitando información de acceso de la cuenta para poder realizar un pago a la empresa,
2. Sujeto pasivo: Dos personas jurídicas,
3. Se individualiza al sujeto activo del delito: No
4. Coautoría: Dos
5. Pruebas: MP no aporto prueba idónea y pertinente, se a porta prueba documental como estados de cuenta,
6. Monto robado: ¢ 11 808 425, esto por cuatro depósitos de: 6 346 750, 640 000, 300 000, 4 521 675.
7. Bancos intervinientes: Cuenta de la víctima Banco Nacional, cuenta donde se acredito el dinero BAC San José
8. Otros: A- apelación se fundamenta en errónea valoración de la prueba, B- tribunal de primera instancia afirma que la acusación del MP presenta defecto de imputación, al no individualizarse las acciones del imputado, C- se utilizaron dos cuentas para recibir el dinero fraudulento, D- la acusación no atribuye al imputado una conducta típica del artículo 217 bis del CP para determinar el dolo, solo el deposito del dinero es insuficiente para acreditar el dolo, E- no se acredito que el imputado fuera quien retiro el dinero, F- imposible condenar por el 365 CPP principio de correlación entre acusación y sentencia,
9. Resultando de Tribunal de Juicio del Primer Circuito Judicial de Alajuela, sentencia 152-2022 de las 11:00 18-2-2022, se absuelve de toda pena y responsabilidad por un delito de estafa informática
10. Resultando Tribunal de Apelación de Sentencia: se declara SIN LUGAR el recurso de apelación de sentencia interpuesto por el representante del Ministerio Público, confirmándose en todos sus extremos el fallo impugnado

Jurisprudencia N° 7.

Delito: Estafa informática

Resolución: 1862-2021

Despacho: Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José

Fecha: 02 de diciembre del 2021 a las 10:05

Análisis:

1. Medio de cometer el delito: Uso de tarjetas clonadas para retirar dinero y realizar compras en comercio,
2. Sujeto pasivo: Banco de Costa Rica, Credomatic
3. Se individualiza al sujeto activo del delito: No
4. Coautoría: tres sujetos,
5. Pruebas: Documental
6. Monto defraudado: ¢ 1 1190 000
7. Bancos intervinientes: Banco de Costa Rica, Credomatic
8. Otros: A- Delito de estafa informática modalidad delito continuado,
9. Resultando de Tribunal Penal del Tercer Circuito Judicial de San José, sede Suroeste, número 301-2021 de las 11:23 del 7-5-2021, se absuelve por certeza DE UN DELITO de estafa informática a: un imputado y por aplicación del principio in dubio pro reo a dos imputados. Por modalidad de delito continuado: un imputado 5 delitos y 5 años de prisión por cada delito, un imputado 1 delito de estafa informática y 5 años de prisión, un imputado 6 delitos de estafa informática y 5 años por cada delito, dos de los sentenciados se les concede el beneficio de arresto domiciliario con monitoreo electrónico.
10. Resultando Tribunal de Apelación de Sentencia: Se declara sin lugar el recurso de apelación de sentencia penal interpuesto por el acusado

Jurisprudencia N° 8.

Delito: Estafa informática

Resolución: 1398-2021

Despacho: Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José

Fecha: 15 de Setiembre del 2021 a las 11:30

Análisis:

1. Medio de cometer el delito: Sustracción de tarjeta de débito y utilización del PIN y con ello engañando al banco
2. Sujeto pasivo: Persona física
3. Se individualiza al sujeto activo del delito: Si
4. Coautoría: No
5. Pruebas: Documental
6. Monto defraudado: ¢ 400 000
7. Bancos intervinientes: Cuenta de la víctima en BCR,
8. Otros: A- defensa presenta apelación, por indebida fundamentación y violación al debido proceso, B- MP acuso por hurto agravado, posterior el ad quem ordeno se conociera y se juzgara por el delito de estafa informática,
9. Resultando de Tribunal Penal del Primer Circuito Judicial de San José, número 447-2021 de las 10:07 del 17-6-2021, pena de 5 años de prisión,
10. Resultando Tribunal de Apelación de Sentencia: Se declara sin lugar el recurso de apelación de sentencia penal

Jurisprudencia N° 9.

Delito: Estafa informática

Resolución: 772-2020

Despacho: Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón

Fecha: 21 de agosto del 2020 a las 15:55

Análisis:

1. Medio de cometer el delito: Ingeniería social, le dijeron a la víctima que facilitara número de cuenta y clave para pagarle por contratarle servicio de restaurante.
2. Sujeto pasivo: Persona física
3. Se individualiza al sujeto activo del delito: No
4. Coautoría: Si
5. Pruebas: Documentales, deficientes para acreditar coautoría
6. Monto defraudado: ¢ 1 220 000

7. Bancos intervinientes: Cuenta de la víctima del Banco Nacional, cuenta donde se retiró el dinero fraudulento Mutual Alajuela
8. Otros: A-representante del MP interpone apelación, alega errónea valoración de la prueba, B- el imputado alega que el presto la cuenta a una tercera persona, C- falta de pruebas, el MP solo presento estados de cuenta del depósito del dinero y no rastreo de llamadas, IP, estudio de movimientos de cuentas antes y después de los hechos del imputado, D- el imputado por su condición humilde presto la cuenta porque es el tipo de personas que buscan las organizaciones criminales,
9. Resultando de Tribunal Penal del Segundo Circuito Judicial de Alajuela, Ciudad Quesada, número 2019-542 de las 08:30 del 25-6-2019, se absuelve de toda pena y responsabilidad al imputado por un delito de ESTAFA INFORMÁTICA,
10. Resultando Tribunal de Apelación de Sentencia: Se declara sin lugar el recurso de apelación de sentencia incoado por el representante del Ministerio Público

Jurisprudencia N° 10.

Delito: Estafa informática

Resolución: 1145-2020

Despacho: Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José

Fecha: 14 de Julio del 2020 a las 10:00

Análisis:

1. Medio de cometer el delito: Incidir en los datos del sistema bancario dando como resultado la obtención de información fraudulenta, con el fin de apropiarse de los datos de usuario y contraseña.
2. Sujeto pasivo: Persona jurídica, Scotiabank de Costa Rica S.A.
3. Se individualiza al sujeto activo del delito: No, la dirección IP se ubica en México Cuernavaca,
4. Autoría: Si
5. Pruebas: Documental, testimonial
6. Monto defraudado: $ 18 000, en tres retiros

7. Bancos intervinientes: Cuenta de la víctima y de donde se depositó el dinero es de Scotiabank
8. Otros: A- Querellante interpone apelación por fundamentación contradictoria, B- se realiza el retiro fraudulento a un cliente del banco, el banco le reintegra la cantidad defraudada, C- se considera que el Tribunal Penal dejó de apreciar circunstancias indiciarias que quedaron debidamente acreditadas y que constituyen juicios hipotéticos de contenido general, cuya valoración integral conforme a la experiencia común, se hacía necesaria para la correcta solución de fondo del caso de marras
9. Resultando de Tribunal Penal del Tercer Circuito Judicial de San José, Pavas, número 1084-2019 de las 11:45 del 12-9-2019, en APLICACIÓN DEL PRINCIPIO IN DUBIO PRO-REO se absuelve de toda pena y responsabilidad a ENRIQUE RAWSON VARGAS de un delito de ESTAFA INFORMÁTICA
10. Resultando Tribunal de Apelación de Sentencia: se anula en su totalidad el fallo recurrido, y se ordena el reenvío de la causa ante el Tribunal Penal de origen, para que, con distinta integración, proceda a resolver lo que legalmente corresponde

Resultado del análisis jurisprudencial

Se aborda el desarrollo jurisprudencial del artículo 217 bis del código penal, en lo relacionado a la individualización del autor o autores del delito de estafa informática, se realiza el análisis de diez jurisprudencias de los Tribunales de Apelación de Sentencia del país, las cuales se comprenden del 2020 al 2023, todas con aspectos del delito de estafa informática, en donde el objetivo del análisis es determinar la posición de los Tribunales de Apelación de sentencia ante la identificación de los autores del delito de estafa informática, así como otros datos de interés para determinar la participación del sujeto autor del delito de estafa informática y con ello determinar la responsabilidad penal del imputado.

El Análisis En Relación Al Medio Utilizado Para Cometer El Delito.

En el análisis de jurisprudencia se logra evidenciar que el medio que mayormente se utiliza para cometer el delito es la ingeniería social, entendiéndose esta como el estudio del comportamiento humano para saber cómo piensa o actúan las personas y posteriormente potenciales víctimas, es a través del estudio del comportamiento que los delincuentes poseen el

conocimiento y la preparación para el abordaje de las víctimas, porque esta aprovecha la confianza que conlleva al error de facilitar datos sensibles de información bancaria.

1. El análisis de las 10 jurisprudencias que comprenden del 2020 al 2023, reflejan los siguientes medios por los cuales se cometieron las estafas:
2. Llamadas telefónicas: cantidad seis, los delincuentes se hacen pasar por representantes de la entidad financiera o del Ministerio de Hacienda, logrando convencer a la victima de facilitar usuarios y claves, una vez dentro del sistema bancario realizan la transacción fraudulenta.
3. Ingreso a paginas falsas de internet: cantidad dos, los delincuentes realizan una copia exacta de la página de internet, la víctima no logra tomar las medidas necesarias para distinguir de una página falsa a la real, cuando ingresa sus datos lo que está haciendo la página es capturarlos, la página le genera error o datos inválidos para que lo vuelva a realizar y con ello los ciberdelincuente capturan más datos.
4. Clonar la tarjeta: cantidad uno, los delincuentes utilizan dispositivos para capturar la información de la banda magnética de la tarjeta y con ello clonarla.
5. Robo de tarjeta y uso de PIN en cajero automático; cantidad uno, la manipulación del cajero automático tipifica el delito de esta informática por que el delincuente incide en la manipulación de un sistema informático.

Se logra evidenciar que la estafa informática es producto en su mayoría de la ingeniería social, procurándose de la poca malicia de la víctima, aunque de eso se trata la ingeniería social, el engañar a la víctima haciéndola creer que lo que está haciendo está bien y con ello procurar un beneficio para el delincuente y un perjuicio para la víctima.

El Análisis De La Jurisprudencia En Relación Al Sujeto Pasivo.

Es la persona que se ve perjudicada con el delito, esto en razón del daño y perjuicio que sufre con su patrimonio, el análisis refleja que, de los diez casos estudiados, el 50% corresponde a personas físicas y el otro 50% obedece a personas jurídicas, en el caso de las personas físicas no se puede determinar el rango de edad porque la jurisprudencia no lo indica, aunque si es una realidad que las personas con una edad avanzada son más propensas a ser víctimas de la estada informática, esto porque no consideran la posibilidad del engaño por medio de ciberdelincuente, siendo lo

contrario que las personas más jóvenes sean más difíciles de engañar en los ciberdelitos, esto por el acceso al internet desde una temprana.

Las personas jurídicas, se debe de entender que para que la estafa informática se produzca en este tipo de personas, al que se estafa en realidad es a una persona física, por lo que podríamos estar ante dos tipos de sujetos pasivos, el primero es al que se le contacta y por medio de ingeniería social brinda los datos y el segundo es el que sufre el perjuicio, bajo este concepto la persona jurídica es la perjudicada en su patrimonio, en el caso de estudio de la jurisprudencia un caso de estafa fue la representante legal la que facilito los datos y se vio afectada la empresa.

El Análisis De Las Jurisprudencias En Relación A La Individualización Del Sujeto Activo Del Delito.

Como concepto de sujeto activo se esboza a todos los sujetos que participan para cometer el delito, esto bajo el dominio funcional del hecho, sin embargo como autor intelectual del delito, o persona que realiza la llamada telefónica, la que capta la información y la que ingresa al sistema informático el análisis refleja que solo una persona fue identificada, con la salvedad de que dicha persona cometió un robo y manipulo el cajero automático, por lo que no hubo una estafa informática por ingeniería social o malware.

La máxima es que los sujetos que cometen la tipicidad del delito no son identificados, la jurisprudencia no menciona las razones por las cuales los sujetos activos que realizan los verbos rectores del delito, es ayuna en esa información, se obtiene la información de que efectivamente en los hechos de denuncia como en el testimonio se habla de terceras personas que son las que cometen el delito, esto sin estar identificadas y mucho menos imputadas.

El Análisis De Las Jurisprudencias En Relación A La Coautoría.

En las jurisprudencias estudiadas se logra determinar que, de diez casos, nueve se cometen bajo coautoría o participación, se excluye un caso que sucedió por robo de tarjeta y manipular el cajero automático, en los demás casos es necesaria una participación, la cual es la acción material de consumación del delito, ósea la disposición del bien que en este caso es el dinero, para ello se toma como base del análisis las jurisprudencias, en donde ya sea por los hechos de la denuncia o la declaración de la víctima, se identifica la participación de más de un sujeto en la comisión del delito, siendo este no identificado e imputado.

La persona imputada es en el 100% de los casos el que se apersona al cajero automático o a la ventanilla del banco a retirar el dinero, este sujeto es relativamente fácil identificarlo, en razón de los controles bancarios sobre el uso de tarjetas y retiros que lleva el banco, estos son los primeros imputados del proceso del delito de estafa informática y en el caso del análisis son los únicos, esto porque no brindan información para identificar a los otros coautores o porque son participes, o del todo no se les puede demostrar el dolo.

El Análisis De Las Jurisprudencias En Relación A Las Pruebas.

Las pruebas en los delitos de estafa informática que se describen en la jurisprudencia corresponden a documental, existe dos jurisprudencias que mencionan prueba testimonial, esta prueba lo que se logra determinar es que corresponde a funcionarios de la policía judicial y personal de la entidad bancaria, en cuanto a la prueba documental, refiere sobre a estados de cuenta, videos.

Es importante mencionar que a pesar de que se habla de direcciones IP, en las diez jurisprudencias se mencionan solo en dos de ellas, siendo una dirección en Costa Rica San José y la otra en México Cuernavaca, en cuanto a la llamadas telefónicas, dos clientes indican que son números del Banco, sin embargo no se realiza una triangulación para verificar la posible ubicación de la llamada, siendo en este caso la prueba principal la documental emitida por la entidad financiera sobre los estados de cuenta y los videos de seguridad, donde se acredita la sustracción del dinero transferido fraudulentamente y el retiro del mismo, esto por parte del único imputado y siendo insuficiente para identificar e imputar demás autores del delito.

El Análisis De Las Jurisprudencias En Relación En Cuanto Al Monto Defraudado.

Los montos defraudados en el análisis se logran determinar que ocurre en colones y dólares, siendo los montos muy variados, que van desde los cientos de miles a hasta los millones de colones, no se logra evidenciar si tras la defraudación la cuenta de las victimas quedo en cero, o si lo defraudado corresponde a cuentas principales o secundarias.

El análisis de las jurisprudencias en relación con los bancos intervinientes, el análisis de la jurisprudencia evidencia se evidencias involucrados siete bancos nacionales, dos bancos privados y una mutual, en la relación con bancos privados y mutual estos tuvieron relación con bancos públicos, siendo estos bancos el Banco Nacional, Banco Popular, Banco de Costa Rica.

El análisis de las jurisprudencias en relación en cuanto a otros datos, por ser analizada jurisprudencia de los Tribunales de Apelación de Sentencia, esta solo surge tras una apelación previamente presentada y aceptada, en donde el motivo principal corresponde a una inadecuada valoración de la prueba y violación al debido proceso, siendo los casos donde el Tribunal de Apelación de Sentencia ordenan un juicio de reenvió solo un caso y confirmando la sentencia en los nueve restantes.

Capitulo V. Conclusiones, Recomendaciones y Propuesta

Conclusiones

Para la elaboración de este trabajo, se planteó como problema de investigación el siguiente: ¿Cuáles son los retos que plantea la individualización de la persona autora del delito de estafa informática?, y para resolver el problema, se llevó a cabo la elaboración de un marco teórico que abarca temas importantes y relevantes sobre el delito de estafa informática, regulado en el artículo 217 bis del Código Penal, los cuales se relacionan propiamente con la individualización del delincuente cibernético.

Para dar respuesta a este problema de investigación, se formuló un objetivo general y tres objetivos específicos, los cuales funcionaron de guía para llevar a cabo la investigación y la solución al problema de la individualización del delincuente de estafa informática.

Objetivo específico número uno

Indagar los factores que contribuyen a la dificultad para individualizar al autor o autores de los delitos de estafa informática con base en la entrevista a profundidad realizada a los informantes claves.

1. Herramientas tecnológicas para la investigación: Aunque el ministerio público cuente con herramientas tecnológicas para investigar, como son programas informáticos, la

realidad es que estos son insuficientes para los delitos de estafa informa, siendo la falta de recurso económico la principal justificación para no mejorar estas herramientas de investigación. Actualmente existen en el mercado herramientas que permiten por medio de inteligencia artificial buscar patrones de comportamiento de internet, que facilitarían la búsqueda de datos dejados por los ciber delincuentes, de igual manera herramientas tecnológicas y rastreo de direcciones IP.

2. Falta de colaboración de las personas imputadas: Los sujetos que son llevados al proceso penal no colaboran con la investigación, puesto que aducen que solo facilitaron la cuenta o hicieron el favor de prestar la cuenta y retirar ellos el dinero, además bajo su derecho de abstención la imposibilitan al ministerio público la obtención de información, siendo más bien que bajo su condición de imputados buscan la manera de acogerse a alguno de los beneficios procesales, En el caso del Ministerio Público utiliza mucho el criterio de oportunidad para lograr obtener información de estas personas imputadas.
3. Tecnología usada por el ciberdelincuente: La tecnología con la que cuentan las personas que realizan los delitos de estafa informática, es muy variada y de fácil acceso, como por ejemplo camuflar números de teléfonos, cambiar direcciones IP y ubicación de estas, siendo estos factores que dificultan la labor de investigación por parte del ministerio público.
4. Proveedores de servicios de internet: En el caso de los proveedores de servicio a través de internet, la información que se obtiene no es fidedigna por su fácil manipulación para obtenerla, como por ejemplo los datos a la hora de abrir un correo electrónico, una dirección IP, también existen limitantes como políticas de seguridad como el correo de Gmail.
5. Astucia del delincuente: Este es uno de los principales retos, puesto a través de ingeniería social y manipulación de sistemas de internet, Los delincuentes se preparan para esconderse a través de la internet y no dejar rastro.

Objetivo específico número dos

Identificar las técnicas de investigación que actualmente se utilizan por medio de la entrevista a profundidad a expertos que estén a cargo de la investigación del delito de estafa informática

1. Activación de radio bases: para tratar de localizar la ubicación geográfica de la llamada
2. Solicitud de levantamiento del secreto bancario: se busca la habitualidad de la cuenta, con anterioridad a 6 meses desde el día del delito y un mes posterior.
3. Intervención telefónica: con la declaratoria de crimen organizado se realiza la intervención telefónica.

Objetivo específico número tres

Determinar por medio de la jurisprudencia costarricense sobre los casos de estafa informática para identificar las dificultades en la individualización del autor o autores de la esta informática.

El análisis de jurisprudencia refleja en su mayoría el método de la ingeniería social para cometer el delito de estafa informática, siendo esto a través de una llamada telefónica en donde la persona que realiza dicha llamada, se identifica como funcionario de alguna institución o entidad bancaria, empezando ahí el uso de la ingeniería social para entablar confianza con la víctima.

Al ser una llamada telefónica con un número camuflado, puesto que las víctimas indican que se trata del número del Banco, es un reto para la individualización de esa persona delincuente, sumado a ello, existe la persona que manipula el sistema bancario y haciéndose con ello traspasos fraudulentos de dinero, estos dos sujetos en ninguno de los casos analizados en la jurisprudencia fueron llevados al proceso penal, esto por los métodos que utilizan para cometer el delito, que son a través de una llamada telefónica y la manipulación del sistema bancario.

La persona imputada en estos delitos, que es la cuenta destino, en las jurisprudencias analizadas, indica que solo realizó el favor de prestar la cuenta, que no tenía conocimiento que se le trasladaría dinero fraudulento.

Las jurisprudencias solo determinan dentro del proceso penal a la persona cuenta destino esto en un 100 % del análisis.

El análisis de jurisprudencia demuestra un factor predominante en la estafa informática, y es el uso de la ingeniería social para acceder a la información de la víctima, esto refleja que la persona delincuente es experta en engañar a la víctima por medio de sus palabras y con ello convencerlo de facilitar los datos de acceso, es algo que no se le puede achacar a la víctima, puesto que es parte de lo que se debe de entender dentro de la especialización del delincuente.

Objetivo general

Analizar los retos que plantea la individualización del autor o autores del delito de estafa informática en Costa Rica del periodo 2018 a 2023.

Se ha logrado demostrar por medio de los objetivos específicos que los retos de la individualización del autor de estafa informática dentro del período comprendido son principalmente las herramientas tecnológicas que requiere el Ministerio público para una adecuada investigación, junto con una reforma a la ley de registro y secuestro

Recomendaciones

Analizado el tema de estudio, que son los retos de la individualización de la persona autora el delito de estafa informática, se sugiere una serie de recomendaciones, las cuales van enfocadas en dotar de mejores herramientas a los investigadores del Ministerio Público y del Organismo de Investigación Judicial, siendo estas herramientas de carácter tecnológico y legislativo.

Como primera recomendación, es invertir en comprar programas tecnológicos que faciliten la investigación y que permitan a los investigadores profundizar en la web para rastrear a los ciber delincuentes, siendo estas herramientas tecnológicas con inteligencia artificial.

Como una segunda recomendación, es la capacitación a los fiscales del Ministerio público, esto para que cuenten con el conocimiento de lo que es útil y pertinente en cuanto aprueba para ofrecer, así como una adecuada redacción de los hechos en la pieza acusatoria.

Como tercera recomendación, se propone la divulgación en medios de comunicación sobre la prevención a la ciudadanía para que no sea víctimas de este delito, trasmitiendo los medios por los cuales los delincuentes acceden a su información, como es el uso de ingeniería social y enlaces de internet de páginas clonadas.

Como cuarta recomendación, es la reforma al artículo 9 de la ley de registro y secuestro, números 7425, en donde se permitiría la intervención telefónica en los delitos de estafa informática sin necesidad de que estos sean declarados crimen organizado.

Estas recomendaciones en un abordaje general, benefician a los diferentes actores del proceso penal, como lo son los investigadores, puesto que contarían con herramientas para la investigación y tratar de identificar al ciber delincuente de una manera más ágil, fácil apoyados en la tecnología, beneficiaría a las víctimas, las cuales se podrían ver resarcidas en cuanto a la acción civil y la acción penal, por cuanto beneficiaría sobre todo beneficia a la ciudadanía, puesto que con mejores herramientas de investigación las personas que cometen este tipo de delitos podrían abstenerse a cometerlos considerando que el sistema penal es eficiente.

Propuesta

Primer propuesta, que el Poder Judicial invierta en el Ministerio Público y al Organismo de Investigación Judicial los recursos económicos para comprar los programas tecnológicos que faciliten la identificación del ciber delincuente en una investigación penal, estos programas deberán integrar la inteligencia artificial para que por medio de ella se logre en un tiempo muy reducido el análisis de datos que permitan a los investigadores la obtención de información que facilite la individualización del autor o autores del delito de estafa informática.

Segunda propuesta, es la reforma al artículo nueve de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, No.7425 de 09 de agosto de 1994, es por parte de la Asamblea Legislativa, en donde se incluya el delito de estafa informática para que pueda ser investigado a través de la intervención de las comunicaciones, quedando el artículo de la siguiente manera:

INTERVENCION DE COMUNICACIONES

Artículo 9- Autorización de intervenciones

Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de los siguientes delitos: estafa informática, secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación, producción o difusión de pornografía y delitos sexuales contra personas menores de edad; trata de personas, tráfico ilícito de migrantes y tráfico de órganos; homicidio calificado, femicidio, genocidio, terrorismo y los delitos previstos en la Ley 7786, Ley sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de Uso No Autorizado, Actividades Conexas, Legitimación de Capitales y Financiamiento al Terrorismo, de 30 de abril de 1998, así como los delitos de corrupción contra los deberes de la función pública que se indican: cohecho impropio, cohecho propio, corrupción agravada, aceptación de dádiva por acto cumplido, corrupción de jueces, penalidad del corruptor, concusión, prevaricato, peculado, malversación, peculado y malversación de fondos privados, enriquecimiento ilícito, legislación o administración en provecho propio, sobreprecio irregular, tráfico de influencias, soborno transnacional, influencia en contra de la Hacienda Pública, fraude de ley en la función administrativa.

En los mismos casos, dichos tribunales podrán autorizar la intervención de las comunicaciones entre los presentes, excepto lo dispuesto en el segundo párrafo del artículo 26 de la presente ley, cuando se produzcan dentro de domicilios y recintos privados, la intervención solo podrá autorizarse si existen indicios suficientes de que se lleva a cabo una actividad delictiva.

Referencias bibliográficas

Acurio, S. (s.f). *Delitos Informáticos: Generalidades*. Recuperado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

AGV. (2024). *¿Qué es una dirección IP y cómo funciona?* Recuperado de: https://www.avg.com/es/signal/what-is-an-ip-address#:~:text=Las%20direcciones%20IP%20funcionan%20como,sitios%20web%20y%20correos%20electr%C3%B3nicos.

Asamblea Legislativa de la República de Costa Rica. (2001). *Aprobación de la adhesión al convenio sobre la ciberdelincuencia. Convenio de Europa sobre Ciberdelincuencia* (Budapest, 2001) N° 9452. Mediante decreto ejecutivo N° 40546 del 3 de julio de 2017, Costa Rica se adhiere al presente Convenio.

Banco Nacional. (2020). *¿INTENTARON ESTAFARLO CON UN NÚMERO TELEFÓNICO PARECIDO AL DE SU BANCO*? Recuperado de: https://www.bncr.fi.cr/intentaron-estafarlo-con-un-numero-telefonico-parecido-al-de-su-banco#:~:text=El%20enmascaramiento%20de%20llamadas%20telef%C3%B3nicas,de%20confianza%2C%20como%20un%20banco.

Belcic, I. (2023). *¿Qué es el malware y cómo protegerse de los ataques?* Recuperado de: https://www.avast.com/es-es/c-malware

Caro, M. (2019). *Aproximación al concepto de perjuicio patrimonial. Revista del Estudios de la justicia.* Recuperado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/file:///C:/Users/Usuario/Downloads/mcoloma,+Gestor_a+de+la+revista,+caro.pdf

Castro, J. (1987). *El Delito Informático*. Revista Judicial, Costa Rica. Año XI, número 41, junio 1987

CIJUL. (2023). *Los Términos Manipulación Informática, Telemática, Electrónica O Tecnológica En El Delito De Extorsión (Artículo 214 Código Penal).* Recuperado de: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/file:///C:/Users/Usuario/Downloads/Los%20terminos%20manipulacion%20informatica,%20telematica,%20electronica%20o%20tecnologica%20en%20delito%20de%20extorsion.pdf

CIJUL. (s.f). *Fraude Informático*. Recuperado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/file:///C:/Users/Usuario/Downloads/fraude_informatico.pdf

Código Penal de Costa Rica. (1970).

Convenio Interamericano sobre Extradición. (1999). Recuperado de: https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=47636&n

Escudero, C.L. y Cortez, L.A. (2018). *Técnicas y Métodos Cualitativos para la investigación Científica.* Editorial UTMACH. Recuperado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://repositorio.utmachala.edu.ec/bitstream/48000/12501/1/Tecnicas-y-MetodoscualitativosParaInvestigacionCientifica.pdf

Flores, I. (2012). *Criminalidad Informática (aspectos sustantivos y procesales).* Recuperado de: https://biblioteca.nubedelectura.com/cloudLibrary/ebook/show/9788490335703

García, G. (2020). *Hablemos acerca de la "Ley Cloud"*. Recuperado de: https://es.linkedin.com/pulse/hablemos-acerca-de-la-ley-cloud-giulliana-garc%C3%ADa-romero

Gorostidi, J. (2020). *LA PLURALIDAD DE VÍCTIMAS DERIVADA DE LA ELEVADA LESIVIDAD EN LOS CIBERDELITOS: UNA RESPUESTA PENAL PROPORCIONAL*. Recuperado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/file:///C:/Users/Usuario/Downloads/Dialnet-LaPluralidadDeVictimasDerivadaDeLaElevadaLesividad-7483941%20(1).pdf

Hernández, R., Fernández C. y Baptista P. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Recuperado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/file:///C:/Users/Usuario/Downloads/Dialnet-Cibercrimen-4639646.pdf

IBM. (s.f). *Que es la piratería.* Recuperado de: https://www.ibm.com/topics/cyber-hacking

INTERPOL, (2024). *Que es interpol.* Recuperado de: https://www.interpol.int/es/Quienes-somos/Que-es-INTERPOL

Interpol. (2024). Desarrollo de Capacidades de Lucha contra la Ciberdelincuencia. Recuperado de: https://www.interpol.int/es/Delitos/Ciberdelincuencia/Desarrollo-de-Capacidades-de-Lucha-contra-la-Ciberdelincuencia

Jovel, C. (s. f). *El documento electrónico, la firma digital y la contratación administrativa.* Recuperado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/file:///C:/Users/Usuario/Downloads/13375-Texto%20del%20art%C3%ADculo-22531-1-10-20140206.pdf

Kaspersky. (2023). *"Empresas que se están digitalizando deben garantizar un entorno seguro:* Recuperado de: *Kaspersky*. https://dplnews.com/mwc-2023-empresas-que-se-estan-digitalizando-deben-garantizar-un-entorno-seguro-kaspersky/

Larocca, N. (2022). Especiales DPL Ciberseguridad. Recuperado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dplnews.com/wp-content/uploads/2022/05/Huawei-transparencia-ante-el-mundo-y-cuidado-end-to-end-para-reducir-el-riesgo-a-cero-ciberseguridad.pdf

Marc Bernaldo. (2021). *Las 15 técnicas de hacking más comunes – ESED*. Recuperado de: https://www.esedsl.com/blog/15-tecnicas-de-hacking-mas-comunes

Merejo, A. (2015). *La Globalización del Cibermundo ITM, Universidad Autónoma de Santo Domingo.* Recuperado de: https://revistas.itm.edu.co › trilogía › articule › downloadta

MICITT. (2023). *Costa Rica Estrategia Nacional de Ciberseguridad* 2023-2027. Recuperado de: https://www.micitt.go.cr/wp-content/uploads/2023/04/Estrategia-Nacional-de-Ciberseguridad-MICITT-2023-2027.pdf

Nava, A. (2019). *Ciberdelitos.* Recuperado de: https://biblioteca.nubedelectura.com/cloudLibrary/ebook/show/9788491901853

Nava, A. (2019). Ciberdelitos. recuperado de: https://biblioteca.nubedelectura.com/cloudLibrary/ebook/show/9788491901853

Orozco, D.. (2011). *Técnicas utilizadas por delincuentes informáticos para realizar fraudes vía medios electrónicos. Facultad Ingeniería de sistemas, Universidad Piloto de Colombia*. Recuperado de: http://repository.unipiloto.edu.co

Poder Judicial de Misiones. (2019). *Cómo detectar y protegernos de los correos electrónicos ... STI - Poder Judicial Misiones Argentina*. Recuperado de https://sti.jusmisiones.gov.ar › sti-web › index.php › 1...

Raúl, R. (2022). *El delito de estafa informática: concepto y casuísticas.* Recuperado de: https://obduliadelarocha.es/el-delito-de-estafa-informatica/

Real Academia de la Lengua Española (RAE, 2020) *Diccionario de la lengua española*. Recuperado de: https://dle.rae.es › engaño

Ribón, E. (2024). *Fraudes Bancarios y Defensa del afectado, nuevas tendencias defraudadoras*. Recuperado de: https://biblioteca.nubedelectura.com/cloudLibrary/ebook/show/9788411976756

Ruiz, R. (2019). *Los problemas del delito de estafa: El "Trile" y otros comportamientos límite. Tesis Facultad de Derecho. Grado en Derecho. Universidad de Valladolid*. Recuperado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://uvadoc.uva.es/bitstream/handle/10324/48044/TFG-D_01233.pdf?sequence=1

Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José. (2023). Resolución Nº 01164 – 2023. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-1187285

Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José. (2022). Resolución Nº 01838 – 2022. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-1139845

Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José. (2021). Resolución Nº 01862 – 2021. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-1065984

Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José. (2021). Resolución Nº 01398 – 2021. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-1052772

Tribunal de Apelación de Sentencia Penal II Circuito Judicial de San José. (2020). Resolución Nº 01145 – 2020. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-987063

Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón. (2022). Resolución Nª 00284 – 2022. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-1083657

Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón. (2022). Resolución Nº 00950 – 2022. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-1119280

Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón. (2022). Resolución Nº 00851 – 2022. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-1113977

Tribunal de Apelación de Sentencia Penal III Circuito Judicial de Alajuela San Ramón. (2020). Resolución Nº 00772 – 2020. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-992095

Tribunal de Apelación De Sentencia Penal. Segundo Circuito Judicial de San José. (2023). Resolución Nª 00256 – 2023. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-1142844

Tribunal de Apelación De Sentencia Penal. Segundo Circuito Judicial de San José. (2023). Resolución Nª 00256 – 2023. Recuperado de: https://nexuspj.poder-judicial.go.cr/document/sen-1-0034-1142844

UCR. (2009). *Especialistas reconocen necesidad de ley sobre ciberdelitos*. Recuperado de: https://www.ucr.ac.cr/noticias/2009/10/23/especialistas-reconocen-necesidad-de-ley-sobre-ciberdelitos.html

UCR. (2023). *Con una mejor cultura digital disminuyen los riesgos de una estafa informática*. Recuperado de: https://www.ucr.ac.cr/noticias/2023/11/08/con-una-mejor-cultura-digital-disminuyen-los-riesgos-de-una-estafa-informatica.html

UCR. (2023). *Observatorio de la Política Internacional. El cibercrimen y su conexión con el crimen organizado.* Recuperado de: https://opi.ucr.ac.cr/node/1974

UNODC (Oficina de las Naciones Unidas contra la Droga y el Delito). (2019). *Cooperación Internacional contra los Delitos Cibernéticos.* Recuperado de: https://www.unodc.org/e4j/es/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

Velasco San Martin, Velázquez Olavarrieta. (2020). *Recomendaciones para abordar la detección del fraude cibernético en México. Recuperado de*: https://assets.publishing.service.gov.uk

Velasco, E. (2019). *Delincuencia Informática*. Recuperado de: https://biblioteca.nubedelectura.com/cloudLibrary/ebook/show/9788413133577

World Compliance Association. (2019). *Cómo la tecnología puede prevenir fraudes*. Recuperado de: https://www.worldcomplianceassociation.com/1561/articulo-como-la-tecnologia-puede-prevenir-fraudes.html

Apéndices

Apéndice A. Cartas

San Ramón, 2 de mayo de 2024

Sres.
Miembros del Comité de Trabajos finales de Graduación
Facultad de Derecho
Grado de Maestría
Universidad Internacional de las Américas
San José

Estimados señores:

Por medio de la presente hago constar que yo, MSc. Carlos María Palma Zúñiga, cédula No. 202260865, filólogo, miembro activo de Colypro, número de carné 3367, doy fe de haber corregido el trabajo final de graduación, titulado "*RETOS DE LA INDIVIDUALIZACIÓN DE LA PERSONA AUTORA DEL DELITO DE ESTAFA INFORMÁTICA*" a cargo del estudiante **JHONNY ANTONIO ROJAS DÍAZ** , con cédula de identidad N.º 205910667, para optar por el grado de Maestría en Derecho, y en relación con los siguientes aspectos:

1. Lexicografía, morfología, fondo y forma en su totalidad.
2. Uso correcto de las preposiciones.
3. Usos lingüísticos de los signos de puntuación, interrogación, exclamación.
4. Los solecismos, barbarismos, cacofonías, anfibologías, monotonía del lenguaje, redundancia, pleonasmo y la ortografía.

Por tanto, doy fe de que este proyecto contiene un fondo claro y preciso de la propuesta expresada en el mismo, con ideas correctas, que mantienen el hilo conductor a lo largo del documento.

Atentamente.

_____

MSc. Carlos María Palma Zúñiga

No. de Cédula 202260865

CARLOS MARIA PALMA ZUÑIGA (FIRMA)
Firmado digitalmente por CARLOS MARIA PALMA ZUÑIGA (FIRMA)
Fecha: 2024.05.02 16:51:36 -06'00'

¡AUTORIZACIÓN DE LA TUTORA

San José, 03 de mayo de 2024

Señores

Instituto de Estudios de Posgrado en Derecho

Universidad Internacional de las Américas

Estimados señores:

Por este medio la suscrita en calidad de tutora comunico formalmente que el PROYECTO DE GRADUACIÓN del estudiante Jhonny Antonio Rojas Díaz, cedula 2-0591-0667, titulado: "Retos de la individualización de la persona autora del delito de estafa informática" cumple con los requisitos para la presentación final.

Hago constar que he revisado y aprobado en el documento los siguientes criterios establecidos por la Universidad Internacional de las Américas.

	Criterio	Calificación asignada	Calificación Obtenida
1.	Cumplimiento de entregas de avance	20%	20%
2.	Coherencia entre los objetivos, los instrumentos aplicados y los resultados de la investigación, proyecto o práctica	30%	30%
3.	Relevancia de las conclusiones y recomendaciones o del producto final del proyecto o práctica	25%	25%
4.	Calidad y detalle del marco teórico	25%	25%

Firmo en San José a las 17:50 del 03 de mayo de 2024.

ODILIE ROBLES ESCOBAR (FIRMA)

Firmado digitalmente por ODILIE ROBLES ESCOBAR (FIRMA)
Fecha: 2024.05.03 17:53:06 -06'00'

AUTORIZACIÓN DE LA LECTORA

San José, 01 de mayo de 2024

Señores
Instituto de Estudios de Posgrado en Derecho
Universidad Internacional de las Américas
S.O

Estimados señores:

Por este medio la suscrita, Dra. Flor Sidey Salazar Fallas, comunico formalmente lo siguiente.

Hago constar que en calidad de lectora del trabajo de investigación titulado **"RETOS DE LA INDIVIDUALIZACIÓN DE LA PERSONA AUTORA DEL DELITO DE ESTAFA INFORMÁTICA"** del estudiante **JHONNY ANTONIO ROJAS DÍAZ, CÉDULA 2-0591-0667** de la Maestría en Derecho con énfasis en Derecho Penal de la Universidad Internacional de las Américas cumple con los requisitos de forma y fondo.

En la calidad indicada apruebo el presente Proyecto de Graduación para optar por el título de máster en Derecho con énfasis en Derecho Penal.

Firmo en San José a las 23:07 horas del 01 de mayo de 2024.

FLOR SIDEY SALAZAR FALLAS
Digitally signed by FLOR SIDEY SALAZAR FALLAS
Date: 2024.05.01 23:10:11 -06'00'

Flor Sidey Salazar Fallas

Lectora

Apéndice B. Entrevistas a profundidad

Entrevista Juez de Tribunal Penal

Archivo de audio

Audio Entrevista Juez de juicio

Transcripción

Orador 1: Jhonny Rojas

Orador 2: Juez de Tribunal

Orador 1

Pongo a grabar en el TEAMS, grabar. Iniciar. Déjeme ver la grabación se ha iniciado.

¿buenas tardes, don Richard, cómo le va?

Orador 2

Muy buenas tardes, don Jhonny, un gusto.

Orador 1

Gracias el gusto es mío, le agradezco el colaborarme para la entrevista en el tema de mi tesis de maestría. De Derecho Penal de la UIA, el tema de la tesis don Richard es “Retos de la individualización de la persona autora del delito de estafa informática”. Para lo cual. Se requiere una serie de entrevistas a profundidad, a funcionarios judiciales que tengan relación con este con los delitos de estafa informática, por lo cual le agradezco mucho su anuencia, ayudarme con el tema para la entrevista. La misma, la misma.

Orador 2

Claro que sí.

Orador 1

Se compone de una serie de preguntas guías. Son preguntas guías en la de las cuales pues se pueden ampliar. Podemos hablar libremente como una conversación fluida del tema, pero la cual sí tiene una estructura que es la que vamos a tratar de cumplir dentro de la medida de lo posible. ¿Entonces, don Richard, cuál es su puesto dentro del Poder Judicial?

Orador 2

Yo soy juez de del Tribunal o este Tribunal Penal, juez de juicio.

Orador 1

Entonces, puedo entender que el supuesto es el que se encarga de realizar propiamente la valoración de las pruebas que recaba el Ministerio Público.

Orador 2

Sí, señor, exactamente.

Orador 1

Perfecto, posee usted, experiencias en delitos de estafa informática Don Richard.

Orador 2

Bueno, la experiencia como tal, no tengo una capacitación específica don Jhonny con el tema de las estafas informáticas, lo que pasa es que, al ser juez de primera instancia, juez de Tribunal Penal, pues evidentemente sí he tenido algunos asuntos relacionados a acusaciones como

estafas con estafas informáticas, que es una modalidad, pues no es bastante nueva, pero que, si vienen, en aumento en cuanto a ese tipo de asuntos.

Orador 1

¿Sí, ahora qué dice usted en aumento en Richard? ¿Qué tan común se ha vuelto a tener este tipo de delitos de estafa informática?

Orador 2

Una estadística base no tengo don Johnny, pero si le digo que conforme a lo que se veía antes, en este tiempo que tengo yo de estar en el Poder Judicial de 25 años, a lo que se ve ahora, pues aumentado significativamente. Tan es así que en un año perfectamente podemos ver de 10 a 15 estafas informáticas.

Orador 1

Claro.

Orador 2

Como asunto, evidentemente, juicio, verdad en la etapa de juicio. Ni qué decir de los asuntos que sé que llegar a conocimiento mío de estafa informática en donde muy regularmente y esa es la problemática que tenemos muy regularmente. el Ministerio Público solicita algún tipo de sobreseimiento o desestimación en relación a estas causas y son abogados particulares los que pues toman la batuta como el tema de ir más allá en las estafas informáticas.

Orador 1

Entiendo. ¿Por qué se produce esta acción del Ministerio público de solicitar un sobreseimiento o un desistimiento Don Richard, en qué radica?

Orador 2

Bueno, mi criterio, mi criterio, es que, al ser delitos de una cierta complejidad, parece que hay es muy recurrente que yo lo diga. Por ejemplo, las apelaciones, que los fiscales y fiscalas salgan con un tema de protocolo de un departamento del OIJ. Ahí tengo, lo tengo lo tengo

Orador 1

De Ciberseguridad

Orador 2

Hay un departamento del OIJ qué hace delitos informáticos que se encarga o que se han cargado de establecer como un ABC con relación a este tipo de delitos de estafas informáticas y a mí me da mucha, o me veo muy curioso que casi todos concluyan con que el usuario el cliente el denunciante dio información sensible y que, al haber dado información sensible, el asunto se para y el asunto no se puede investigar. Va, o sea, lo estafaron, sí señor, pero porque usted dio su clave, porque usted dio cierta información y en base a esa información es a usted, le ocasionaron el perjuicio, y hay asuntos que no, hay asuntos que incluso uno llega hasta sospechar, y lo digo con toda la objetividad del caso, que hay como hasta sobre todo en entidades financieras, que hay como una especie de una red en donde hay funcionarios internos. Evidentemente eran entidades bancarias de repente involucrados con esa situación. Es lo que es lo que me llama la atención y casi siempre al menos yo devuelvo mucho a la etapa de investigación, a la etapa del Ministerio público para que se hagan todas, absolutamente todas las diligencias pertinentes. Hay asuntos en donde se ubica la persona, saben que el número le pertenece a fulano de tal y esto o lo otro, pero di siempre piden un sobreseimiento o desestimación porque utilizan el argumento de que se dio información sensible.

Orador 1

Entiendo. ¿Entonces, de los delitos o de los procesos que si llegan a juicio don Richard? ¿Cuál cree usted, desde su puesto? ¿Cuál es el medio que utilizan más los delincuentes para estafar, llámese llamadas telefónicas, mensajes, mensajes de texto, páginas de Internet? ¿Cuál sería el medio que más utilizan?

Orador 2

El método que más utilizan es el de la famosa llamada telefónica, lo hemos visto hasta con Personeros o con personas que están privadas de libertad. El segundo método que más utiliza es el tema de las páginas, las páginas de Internet, el tema de las compras, por ejemplo, que se hacen mediante Internet, el tema del depósito de esas en esas situaciones y que, pues no hay, no hay garantía de que ese depósito de que esa página o que esa persona que está del otro lado de Internet, pues evidentemente vaya a cumplir con ello, en el tema de la llamada telefónica tiene, he es cierto que es la primera por cierto, tiene cierta en situación de vamos a ver, de habilidad, del que llama para con la persona que responde, es decir, más o menos sacamos alguna estadística en cuanto a edad de personas que resultan ofendidas, generalmente son personas adultas mayores, personas adultas mayores que tienen, pues evidentemente, alguna tarjeta débito, alguna cuestión de la atención y esas personas están, por qué no decirlo don Jhonny, desde cierto punto vulnerables en el tema del manejo de esas intenciones, entonces hay como una especie de vulnerabilidad en relación a estas personas con la llamada telefónica. Ahora a los que bueno no me considero yo, es tan joven, pero los jóvenes jóvenes de ahora es muy difícil que les hablen de una estafa informática por medio del teléfono. De llamada telefónica, conocieron son los adultos mayores que son están más expuestos insisto, a que se dé la situación de estafa promedio del teléfono, que para mí la primera, que la segunda es el tema de las páginas electrónicas.

Orador 1

¿Claro, considera usted don Richard que esos delitos se realizan más de una forma individual o en coautoría?

Orador 2

Hay algunos que sí se hacen de manera individual, que son los de las páginas de Internet, hay una página, que ofrece la venta o la compra de algo y nos vemos en tal lugar y bueno, todo eso verdad, pero cuando se hace por medio de llamada telefónica, yo sí entendería que hay algún tipo de coautoría de que hay alguna especie de red, que hay alguna especie de conexión y ahora lo dije, Johnny, de repente son personeros del mismo banco, o de la misma empresa financiera que pone sobre aviso de ciertas situaciones, porque cuando pasa el tema de llamada telefónica. ¿Cómo se sabe que esa persona maneja cierta cantidad de plata en sus cuentas? ¿Cómo se sabe que esa persona tiene x cantidad de tarjetas? O sea, información que sí de repente es sensible pero no porque provenga de quien está haciendo estafado en ese momento, sino porque quienes eventualmente trabaja en esas entidades financieras tienen acceso a esa información sensible y la dan a otras personas, hay incluso financieras o entidades de estas que antes don Jhonny lo digo porque tengo bastante tiempo de estar en eso. ¿Llegaban a sacarle copia o fotos al a los libros de entrada? Y ahí tenía a todas las personas que eran eventualmente llegaban a algún proceso, llámese juzgado contravencional o juzgado civil, les sacaban copias y no recuerdo el nombre, concretamente don Jhonny, pero que utilizan en almacenes de línea blanca, que tenían un registro de ellos, se decretó en algún momento inconstitucional, pero que tenían una información ellos, se me olvida el nombre insisto, ellos se metían ahí como soltaban y determinaban sus deudas, ósea, información que viene a ser sensible, un número de expediente y todo, esos aparecen con un asunto que en civil en tal lado, después aparece con otro asunto. Y es que se encargaban de ir a sacarle copia el libro de actas al libro de Entradas. Perdón, que era un libro bastante grande, ahora pues se hace diferente, me imagino. Ya que todo es más que todo es más electrónico, es una forma de ellos de tener esa coautoría y que no hablemos solamente de una persona.

Orador 1

¿Exacto, y considera usted que a la hora que se eleve a juicio se llevan a todos los responsables al mismo don Richard?

Orador 2

Bueno, las investigaciones que yo he visto, al menos materialmente, sí. No creo que señale los responsables, por ejemplo, de una entidad financiera, pero la última que tuve que fue hace como un par de meses y recuerdo que la persona e hicieron, o sea le sacaron el dinero a una Junta directiva y lo distribuyeron en diferentes personas. ¿Es extrañísimo, ¿verdad? Distribuyeron el dinero en diferentes personas que generalmente en locales comerciales. Me llamó la atención que uno de los señores del local comercial devolvió el dinero, porque él dice que sí, que efectivamente le llego la plata. ¿Yo no sé si el señor había hablado con alguien de sobre un pago que le iba a llegar algo bien, se quedaba como una parte, estoy especulando verdad? Se quedaba con una parte y devolvía otra y es una manera de justificar por qué me ingresa x cantidad de plata en mi cuenta. ¿Por qué? ¿Pues yo trabajo en electrónica? ¿Por cierto, ahora, si yo trabajo en electrónica me llegó un pago de 1 600 000 pago de X cosa, ¿verdad? Pero eso hablamos de esta posibilidad de la pregunta anterior. Pago de x cosa y cuando llega la persona no me das que pago de lo que quedamos ese 1 600 000, que vos te quedas con 300, el dueño del local se queda con 300 y entrega 1 300 000. ¿Entonces presta y es de una forma hasta de blanquear, verdad, el tema del dinero, por eso hablo de la coautoría, pero sí esa investigación, al menos puntualmente, sí decía los puntos donde se fue a distribuir el dinero y quién lo distribuyó? ¿O al menos de qué cuenta se distribuyó, cuándo se sacó? O sea, se hace una especie de seguimiento, mapeo con relación al dinero cuando se sacó cuando ingresó el tema de los montos, ahora acabo de ayer un día de estos, una estafa informática, igual los dineros sacados de una cuenta. ¿Vienen todos los montos debidamente saturados? ¿Quién fue el que sacó el dinero? ¿Por qué tenía? Ella, ella acceso a esa cuenta que es una, es una tía con una sobrina y le saco casi que 5 000 000 de colones en 2 años, 3 años de una cuenta de manera fraccionada o sea sacaba 50 mil, 40 mil, 50 mil, 40 mil, y bueno, este ahí sí se determina, sería un mapeo para mí hay un mapeo adecuado en relación a quienes al menos tenemos donde, del trasiego de los dineros. Lo que no hay don Johnny es, por ejemplo, quien da la información en el Banco. ¿Lo que no hay es quién es el que está del otro lado, en el Banco o en la entidad financiera y dar la información ¿verdad? Porque nos llama mucho la atención en estafas informáticas en donde, por ejemplo, las personas recibe hoy 5 000 000 en la cuenta de x pago de algo, una venta de algo y que a los 3 días estén llamando a esa persona a ver si pesca en algún tema alguna situación, ¿verdad? ¿Cómo saben ellos, cómo saben que esa persona acaba de recibir 5 000 000? Bueno, es que alguien del Banco tuvo que haberle dicho e insisto, a veces se da, a veces no se da, se lo digo por el conocimiento, no porque hayamos un asunto acusado, pero sí se nos han presentado asuntos en

donde nos comentan. Es que a mí me depositaron esa cantidad a tal cuenta que a los 3 días me estaban llamando para intentar hacerle una? Yo creo que todos hemos ido en algún momento. ¿Candidatos a que nos estafen por teléfono, verdad?

Orador 1

Claro.

Orador 2

Me parece a mí. ¿Entonces, cómo saben que uno sí tiene cierta cantidad hasta la cuenta? A veces batean, a veces batean, pero hay otras veces en donde sí. ¿Efectivamente, uno se queda pensando, pero cómo saben? Bueno, ahí es donde está esa persona que generalmente no aparece en una cosa así.

Orador 1

¿Claro, y también don Richard, trayendo uniendo todo lo que hemos conversado del tema de la llamada y el tema del informante, podríamos decir, o supuesto informante está la persona que realiza la llamada y obtiene los datos de la víctima? ¿Y traslada ese dinero a una cuenta? Que en muchos casos son personas que las prestan inocentemente o ingenuamente, entonces esa persona que realiza o toda esa estructura fuera de la persona que recibe el dinero, muchas veces o también de su experiencia, se sientan en el banquillo del acusado.

Orador 2

No, generalmente no, en el caso que te contaba ese señor que recibe el 1 600 000. ¿Y que los devuelve, porque los devuelve, Eh? Por eso te habría que yo especulaba de que posiblemente le dijeron vas a recibir 1 600 000, si usted si usted los recibe y me los entrega. Te devuelvo 300 te devuelvo 200, te devuelvo 200 o 300 000 sin necesidad de hacer absolutamente nada, pero todo ese engranaje del de que te depositó, porque te lo dije ahora, don Johnny, hay personas que son

muy hábiles para el verbo. ¿Tengo un verbo muy hábil, verdad? Tienen una una buena comunicación, una facilidad de comunicación, pero de repente en el tema tecnológico o informático no son tan diestros. Entonces puede que la persona está hablando con usted y que este y que te tenga en altavoz y que realmente el que sabe cómo hacer la consumida informática es otra persona, verdad? ¿Y esa persona pues posiblemente no va a figurar el que va a figurar de donde sale la llamada o quien habló con usted? Definitivamente, para mí actúan otras personas. Lo que pasa es que identificarlas, al menos solo las que puntualmente se hacen los depósitos. ¿De dónde salió la llamada? ¿De qué teléfono a personas? A esta persona que te den es un asunto complicado porque ya ahí yo puedo tener un teléfono que no es a nombre mío, que sea a nombre de otra persona perfectamente consiguiendo un chip para llamadas, inventarme un número de cedula no es rigurosidad en esos temas, no hay rigurosidad para tener un chip, utilizar un chip que no esté mi nombre no hay rigurosidad, que son aspectos a mejorar.

Orador 1

Claro, y lo mismo ocurriría don Richard con las páginas falsas de Internet que captan datos lo mismo.

Orador 2

Las páginas falsas de Internet yo tengo la solución en mi mente con respecto al tema de las páginas falsas en Internet. Para mí, cuando se crea una página cuando crea una página. ¿Que se va a dedicar a la venta de cuestiones al tema comercial? Para mí debería estar inscrita. Como como hacen en X en la aplicación esta X que la persona supuestamente famosa tiene una palomita, creo que un color azul o tiene palomita, no tiene algo de color azul que demuestra que la efectivamente es de esa persona. ¿Lo hacen con los famosos, verdad? Lo hacen con las personas famosas que usted distingue, que no se da cuenta diferente porque tiene esa situación, que eso lo controla. X verdad, que es la anteriormente Twitter. A mí me parece que en el tema de las páginas electrónicas debería ser exactamente igual por Facebook que Facebook. Legitime que esa esa IP porque es un IP al final es el de Richard White, que se dedica al tema del comercio. Para que si se vende o se compra o se estafa mediante esa cuenta, pues evidentemente los responsables sean Yo, se ha

Richard White, el dueño de la cuenta que se creó un Banco, que se creó, un Banco de cuentas que se dedican al tema comercial y evidentemente quien tratar bajo su propio riesgo Don Johnny, como una persona que no tiene una cuenta oficial de venta y comercio, pues diay es bajo su propio riesgo, porque usted y yo podemos hablar con por por Messenger, podemos hablar por Facebook. Y mira, si tienes unas llantas que me gustan, esa te las compro, tienes y pero ahí es mi responsabilidad. Ah, quiero unas llantas conseguirlas en Facebook que de segunda unos aros algo así, ingrese a una página oficial que esté debidamente registrada, oficializada por Facebook, y yo tengo ahora seguridad y certeza que estoy tocando como una página comercial y que yo no responsabilidad en el tanto a mí no se le entreguen lo que yo estoy pidiendo.

Orador 1

Correcto, entonces podríamos deducir un Richard que esa falta de o más bien de control de los IP, sería un obstáculo para identificar al ciberdelincuente.

Orador 2

El control. Es correcto, pero ese es el obstaculo más grande. A veces la persona que le que lo utiliza, el que lo utiliza en el IP llega y ni siquiera sabe de qué están hablando y dice no, no en qué momento y hay una libre. Hay un tema de responsabilidad. Hay. Facebook, hay páginas de Internet o computadoras más que páginas. ¿Que son familiares? Las usa el hermano, la hermana el tío, El papá, la abuela a todo mundo las utiliza. Y es el mismo IP. ¿Entonces, cómo determinados de que de ese IP salió realmente esa situación? Si hay un tema de de personas que les controlan hasta el celular. Y que tenga el Facebook en donde dice familia White, por ejemplo, y están todos y todos son gratis. ¿Y cómo sabemos que en ese momento, recordando que el derecho penal es personalísimo, cómo sabemos que lo utilizó Richard en ese momento, si no fue Germain, si no fue Michel, si no fue mi esposa, cómo sabemos a quién indilgamos responsabilidad, sí, sí esa es la computadora, ese es el IP, pero cómo le indilgamos culpabilidad? ¿1 cómo lo sabemos realmente? Eso es un obstáculo también. Entonces el tema es registrar la página en ese Banco de registro de páginas oficiales que se dedican a la venta y al comercio. ¿También es un tema como el de las sociedades anónimas, Johnny, que dice que para cuestiones judiciales y extrajudiciales, fulanito de

tal verdad? Bueno, ese es el que hay que comunicar y ese es el que se tiene que defender. La actividad genera un riesgo bueno, está bien y vea que. Ustedes están aquí chiquillos. Fulano tendría computadora es mi IP, pero lo que ustedes hagan responsables soy Yo, eso genera responsabilidad y al generar responsabilidad, pues evidentemente. A la hora de identificar a una persona por medio de una estafa, para lo que es una estafa informática, serían muchísimo más fácil el tema investigativo y también el tema de responsabilidad para indilgar responsabilidad.

Orador 1

Claro, y eso aplicaría para el tema de que se haga algo universal para el delincuente que está en Corea poderlo identificar y tener ayuda de la Cooperación Internacional bajo el Convenio Budapest.

Orador 2

¿Perfecto, perfectamente, perfectamente un tema de unificar que tienes a nivel internacional, porque lo que usted dice es muy cierto, ya ni las estamos, a veces vienen de Tailandia, verdad? Vienen de de de países que están en una zona honoraria casi que 8 o 9 horas más que nosotros y diay cómo identificamos a la persona, ahora tenemos una situación, esto genera esto, es una es una real desconfianza.

Orador 1

Ha hoy don Richard, podríamos decir que identificar al autor intelectual de una estafa informática sería imposible.

Orador 2

No, no, no, no, no es imposible, pero sí se tiene que dar muchas colaboración de las personas que eventualmente es la que llama a la persona que realmente es la que ejecuta actos, actos, materiales, o sea, la la persona que que ya empieza con los actos de de ejecución, tiene que haber

colaboración de esta para determinar quien es el famoso autor intelectual de una situación que nos ocupa. ¿En principio es complicado, verdad? En principio es complicado porque, por ejemplo, voy a utilizar mi experiencia personal, mi conocimiento privado. Bueno, un día me llama 2 o 3 de la mañana y me dicen que hay en la persona, allá en Tailandia. Por cierto que me que me hizo un intento de bueno que hizo la compra de mi tarjeta, por 150 dólares, después se hizo otra por 700 dólares y después hizo otra por 1000 y resto de dólares. Y que el Banco al al sentir que era algo sospechoso lo que la tarjeta y obviamente no autorizó la compras, bueno. ¿quién era? ¿Cómo quién era esa persona ahí en silla Jhonny, ahí resulta materialmente imposible? poder determinar. ¿Quién era esa persona que estaba haciendo esos esos movimientos? Al menos no se lo comunicó exactamente, nada más se veía y que era de ese país y que era a esa hora de la noche, pero yo tuve suerte de que de que en el Banco estaba como quien dice advertidos y hay un componente Johnny también que tenemos que utilizar y el componente a como estamos en el tema de peligrosidad, tenemos que poner de nuestra parte, tenemos que ser desconfiados, tenemos que ser altamente desconfiados para que de ahí es donde no hay Poder Judicial, no hay investigación, no hay protocolo que venga a solventar el cuidado personal que tenemos que tener con nuestra seguridad en temas, en temas informáticos, ¿Porque de verdad hay asuntos, hay asuntos don Johnny, en donde la persona da la clave? En donde la persona da la clave, donde la persona da datos sensibles. ¿Y qué hacemos cuando alguien ya cuando alguien ya da los datos sensibles, cuando da la clave, cuando da la información relevante, qué hacemos en ese caso? ¿Es complicadísimo, es complicadísimo porque también hay un ámbito privado en donde bueno, usted le dio la clave? Y no sabemos exactamente de qué se estaba hablando en ese momento, incluso. Yo diría y tal vez estoy hilando muy delgado don Johnny, Yo sé que estamos en el tema de estafa informática, pero si usted y yo pactamos. ¿Que lo voy a comprar por medio de una red social que lo voy a comprar? ¿Algo que usted está ofreciendo vender? ¿Y yo lo veo, usted me ve así? Estamos en esta entrevista y usted no me cumple con lo que yo le pagué, será una estafa informática? ¿Realmente no estaríamos ante ese tipo de penal o estaríamos ante un incumplimiento contractual que evidentemente tiene que ir a la vía civil, será que tiene que ser en la vía penal? Porque la estafa informática no se aleja del componente aquel verdad que tiene que tiene la estafa del 216, el famoso ardid, el engaño y el perjuicio económico. O sea, está bien, no se alejan hacerlo informática de derecho y no hay tentativa Informática, ¿Pero insisto, será realmente que estamos ante una estafa informáticas, o ante un incumplimiento contractual? Tengo ubicado a Johnny, el me tiene ubicado

a mí, don Jhonny nos vemos tal día deposítenme de los aros Yo se los voy a tener Yo se los mando. ¿Serán realmente una estafa informática? ¿O será un incumplimiento contractual? Será que aplicamos bien, que el Derecho penal es la última razón, la última ratio y nos vamos hacia el principio tan importante o nos dejamos porque ese populismo punitivo que existe de que todo va para todo, va para el área penal, todo es penal y hay que penalizarlo todo. Bueno, ahí la dejo, verdad, sin hacer polémica.

Orador 1

Claro, don Richard me surge una pregunta más a raíz de lo que me ha conversado es. ¿Qué tanta, qué tan activa es la colaboración sujeto material, el que retira ese dinero. ¿Qué tanta la colaboración de él para identificar al autor del delito?

Orador 2

¿No le entendí la pregunta, Johnny, vamos a ver, pero usted me habla del sujeto material, a qué no se refiere?

Orador 1

La persona que va al cajero y retira el dinero.

Orador 2

Yo diría que es poca la colaboración que esa persona da. Es poca la colaboración porque la persona sabe que es un dinero que no es bien habido. Un dinero que no proviene de alguna situación legal. Colabora poco. Lo que pasa es que en la condición de testigo imputado, o imputado sospechoso o de testigo sospechoso, no le podemos pedir a él que de información sobre la situación que se está presentando hay una limitación procedimental para poder llegar. ¿para poder pedirle colaboración a esta persona? Insisto, no sabemos si él solamente está prestando la cuenta o se está prestando para sacar el dinero de la cuenta o realmente es parte de todo ese, de todo ese engranaje.

En cuanto a la. Organización criminal que se dedica a ese tipo de situaciones. ¿Entonces muchos no podemos esperar en principio de este autor material que retira el dinero, verdad? O sea, no mucho podemos esperar y a veces también. Pensando positivamente, aplicando ese principio de inocencia del artículo 89 constitucional don Jhonny de bueno, a mí me dice, usted, amigos, Mira, Richard toma, vaya y me saca una plata de tal cajero. Y me la Traes y me haces el favor y resulta que es la plata que proviene de una estafa informática. Esto va y saca el dinero. Es que el hecho de sacar el dinero del Banco no necesariamente nos indica que esa persona es autora responsable del delito de estafa informática, que esa persona es la autora intelectual o que esa persona está dentro de esa red criminal. No nos dice nada. No nos dice mucho si nos dice objetivamente de que fulano de tal fue a sacar el dinero. Pero habrá que escuchar por qué lo fue a sacar. ¿Y cuando le preguntamos a una persona que por qué lo fue a sacar? Nos tomamos el riesgo de perder la información que tiene derecho de abstener. Tiene derecho de exención, evidentemente que no tiene la obligación de decirnos o de informarnos nada.

Orador 1

Correcto. Don Richard le agradezco mucho su tiempo y toda la colaboración que me brindó con esa entrevista.

Orador 2

Con todo gusto, Johnny, estamos a la orden. Cualquier situación que requiera me avisa y con mucho gusto conversamos. No hay ningún problema. Tú sabes que fuimos compañeros, de ahí vamos a seguir en pendientes

Orador 1

Claro que sí, muchas gracias.

Entrevista Defensora Pública

Archivo de audio

Entrevista defensora

Transcripción

Orador 1: Defensora Pública

Orador 2: Jhonny Rojas

Orador 1

Buenas noches.

Orador 2

Le agradezco mucho el colaborarme con esta entrevista para mi tema de maestría de derecho penal de la UIA, que es "retos de la individualización de la persona autora del delito de estafa informática", para la cual me he planteado la recopilación de información de personeros del poder judicial. Para poder abarcar la pregunta y los temas de investigación, entonces le agradezco mucho.

Orador 1

Con muchísimo gusto a las órdenes.

Orador 2

Gracias. Vamos a hacer una serie de preguntas que van a funcionar como una guía dentro de una conversación fluía del tema de la tesis como tal. ¿Entonces, para iniciar, podría indicarme licenciada cuál es su puesto entre el poder judicial?

Orador 1

Sí, Claro, con muchísimo gusto. Bueno, yo soy defensora pública dentro del poder judicial. Me desempeñé en materia penal por espacio de 6 años.

Orador 2

Perfecto y en este espacio que litigo perdón de hizo la defensa en penal. ¿Posee algún tipo de experiencia de delitos de estafa informática?

Orador 1

¿Correcto? ¿Sí, atendí unos, varios, unos 5 delitos, unas 5 ocasiones, procesos, eso sí, en etapa de inicio, verdad? Lo que fue para procesos o más bien diligencias de Indagatoria.

Orador 2

Perfecto. ¿Qué tan común era atender este tipo de delitos, licenciada?

Orador 1

Bueno, atreves de mi experiencia, digamos de las zonas en las que yo me desempeñé, era muy usual en lo que era el área metropolitana, sobre todo sobre todo tuve contacto con esos delitos en la zona de San José. No es tan habitual como el resto de delitos de de de ordinario, verdad, pero este sí sea uno que otro. Es relativamente frecuente, pero no vamos a ver, no, no, no diría que es frecuente, diría que que es poco, digamos, pero sobre todo en esa zona de San José. Es que de pronto uno tiene más contacto con el tipo penal.

Orador 2

¿OK, podríamos decir que entonces el esa aglomeración de personas en la capital? Es donde más se produce ese tipo de delito y saliendo del área rural.

Orador 1

Es que lo que pasa es que es particular, digamos a través del ejercicio. Uno entiende que cada zona. ¿Tiene sus delitos, verdad? Entonces este así como cuando uno se desempeña en el área de Puntarenas o en las zonas costeras. Vemos delitos de navegación u otras particularidades que no tenemos, evidentemente en el área metropolitana es como como que cada zona se caracteriza por los tipos penales o el tipo de delincuencia o la actividad delincuente que hay en cada zona. Entonces yo considero que sí, que lo que es el delito de estafa, sobre todo esa estafa informática, es muy propia de la zona de la zona central, digamos.

Orador 2

Entiendo, Claro. Dentro de su experiencia. ¿Cuál cree usted que es el medio que más se utilizó para cometer el delito de estafa informática entiéndase llamada telefónica mensajes o páginas de Internet fraudulentas?

Orador 1

Vamos a ver en cuanto a las atenciones. Yo. Johnny, en este sentido, digamos de lo. Fueron estafas. ¿Fue propiamente con cuentas bancarias, verdad? Y por medio de solicitud de favores, es decir, en los en los 5, en las 5 ocasiones que yo atendí a un delito de estos era precisamente porque. ¿Tenía una persona y le solicitaba otra colaboración para que le prestaran las cuentas bancarias, verdad? Argumentando que que les iban a depositar un dinero, que les estaban ayudando y que ellos no tenían cuenta en el banco y que entonces de esta forma este instrumentalizaban a otra persona, verdad que no tenía absolutamente nada de conocimiento y en esa cuenta esa persona se depositaban los dineros y eso es lo que yo puedo decirte, que fue la forma más habitual que yo vi.

Orador 2

Por supuesto, Claro, esa. ¿Bajo esa modalidad que usted me está indicando, entonces podríamos indicar que hay un autor o posibles autores detrás de ese delito de estafa informática?

Orador 1

Claro, Claro, básicamente son las personas realmente que cometen el delito. Sin embargo, lo que es la teoría, verdad, desde mi posición de la fiscalía, es que este se consuma a través de estas terceras personas. ¿Verdad que son quienes finalmente disponen verdad del dinero? Pero básicamente no son los los autores intelectuales de de del delito como tal.

Orador 2

Claro. ¿Cuál es la posición? ¿De esas personas, en el momento que se realiza la acusación en el sentido, hay una anuencia a colaborar? ¿A indicar si que fueron engañados o percibe usted que hay un ocultamiento de esos posibles autores?

Orador 1

¿Vea, lo que pasa es que podría decirnos 50/50 hay como gente que no quiere, pero sobre todo bueno, más bien 75/25, verdad? Porque la mayoría de las personas este. Mira esto, esto es abuso de confianza. Entonces brindaron muy propio del costarricense. En los casos que yo te cuento brindaron como la colaboración. a una persona que no se sabe ni los apellidos, que ya no trabaja en la empresa o que ya no tienen contactos cercanos con esa persona, les hicieron el favor, los presionaron, corrieron, sacaron el dinero. ¿Incluso de las personas que yo atendí, ninguna se vio beneficiada, verdad? Bueno, al menos eso decían. ¿Y por su su situación emocional, verdad? Muy de conmoción. Porque son personas que incluso no tienen antecedentes penales ni nada, solo que brindaron esa colaboración. Un poco de la negligencia. ¿Verdad de entender que una cuenta bancaria es como una Cédula? ¿Eso no se le presta a nadie, verdad? Digamos. Y entonces la gente cree que es como como un favor que se puede hacer, que no pasa nada, se se se pone como medio de la cuenta bancaria y entonces de un Estado de mucha. ¿Insatisfacción, verdad? Es personas en un estado emocional. ¿Ve, era, era devastador, verdad? Porque entonces bueno, porque yo estoy

aquí, bueno, estás haciendo procesado por un delito, pero en qué momento yo cuando yo nunca verá, pues ya de pronto a otro ya empiezan como a refrescarse la memoria. Y dice, bueno, pero es que yo le presté, pero esa plata no fue para mí, yo solo él me dijo que es que me presionó, me presionó, que ocupaba que fuera hoy, que hoy mismo, que que se la sacara, ya que es que lo otro. ¿Y yo solo corrí y fui, pero incluso eran compañeros de trabajo que nunca más volvieron a ver, pero entonces? ¿Aún y cuando quisiera colaborar, no tenía ni los medios, o sea, ya ni siquiera sabían cómo se llamaban las personas, verdad? En algunas ocasiones, sí.

Orador 2

Claro, fueron instrumentos en el delito para. La para la ejecución de ese acto material de la de sacar el dinero como tal. Sí, qué lamentable verdad esa esa situación con esas personas.

Orador 1

esas cosas son muy tristes. Que uno se topó usualmente con gente muy honrada que. Que solo Brindó le solo hizo una colaboración, verdad, y por eso es preciso esas esos comportamientos de confianza.

Orador 2

¿Claro, a nivel Claro, a nivel de defensa pública, licenciada, existe algún procedimiento para los delitos de estafa informática?

Orador 1

¿Como procedimiento como tal, no verdad? ¿Tenemos que entender que la defensa pública, los que se desempeñan en materia ordinaria, verdad que es este? Básicamente uno atiende cualquier tipo de delito, verdad de penal adulto. ¿Entonces uno sí tiene como un protocolo verdad de lo que realizaron la indagatoria de evidentemente procurarse brindar toda la información a la persona que se está atendiendo, velar por todas las garantías, verdad? El ejercicio correcto y una defensa técnica.

¿Pero digamos en los derechos de informática a uno lo que le dice es de brinde la información de la persona que tiene que ser del de los datos de esto, verdad? Con una actitud colaboradora con respecto a desenmascarar a esta persona que. Que verdaderamente. ¿Es quien realizó todo? Sí, exacto, más bien que lo que huecó, digamos de pronto o no sabemos si es el autor, porque este a veces también, ni siquiera estas personas vienen a ser los autores. Oiga, pueden ser perfectamente cómplices. ¿Nada más que evidentemente que para poder hacer todo lo que es el traspaso de los dineros ya tiene que haber un conocimiento técnico, verdad? Porque es toda la estafa.

Orador 2

Claro. ¿Entonces podemos o qué o qué concepto tiene usted de? Bajo esa participación o colaboración que brindan las personas imputadas. ¿Se puede o no es suficiente para llevar a los autores intelectuales de delito de Estado informática al proceso penal?

Orador 1

Por supuesto que no. A mí me parece que la fiscalía ahí comete un error, digamos en mi caso la investigación, porque no es mejor. ¿En lugar de traer estas personas e indagarlas como imputados para que de una vez se cojan a su derecho de abstención, no sería mejor tenerlos como testigos? Es y abordar a estas personas como testigos y que brinden la información de las personas que son las que los indujeron. Error para. Verdaderamente intentar atrapar a quienes realmente está cometiendo el delito. Verdad como tal a la mente criminal. Entonces pierde la posibilidad usted indagando a una persona y diciéndole que es el autor responsable de la Comisión o la consumación del delito de estafa, mejor se investigara a estas personas, se les toma participación en la investigación para que éstas los redirijan a quien verdaderamente es la mente, la persona, el autor intelectual no creería yo que sería muchísimo más efectivo. Que, al fin y al cabo, venir a indagar a una persona. Que no tiene nada que dar en el delito, que básicamente fue instrumentalizada y que terminemos sobre seguimiento. ¿O no?

Orador 2

Concuerdo, por supuesto.

Orador 1

Claro.

Orador 2

Sí, licenciada. Como parte de las recomendaciones, así como esta que me acaba de indicar de. ¿De traer a esta persona como testigo, qué otras recomendaciones considera usted que serían importantes a tomar en cuenta para la identificación del ciberdelincuente?

Orador 1

Sí, básicamente lo que yo considero es como en ese tanto, buscar la información. Apetecerse de conectarse básicamente con las entidades financieras, que son verdaderamente quienes pueden controlar y filtrar la no comisión de estos delitos. Bueno, es que. Los bancos también tienen toda la corresponsabilidad en esos tipos de estafas. Bueno, en el caso que estamos hablando en específico. Porque hay un montón de medidas de seguridad que ellos podrían implementar que sí vuelven mas engorroso cualquier trámite, pero evidentemente podíamos. ¿Evitar para todo ese tipo de actuaciones es muy fácil venir a trasladar la responsabilidad a la ciudadanía, verdad? O a esas otras personas que básicamente incurrir en en en procesos más onerosos, considero yo. ¿Entonces porque a nivel de fiscalía, a nivel de poder judicial, de qué forma, si todo eso se hace desde un servidor, de qué forma vas a individualizar? ¿De cuál servidor se está haciendo la gestión? Considero yo que el poder judicial no tiene las herramientas para verdaderamente abordar. ¿Ese tipo de delitos? Eso es lo que yo pienso, digamos ahora. Actualmente hay otras prácticas que que incluso se dejan consignadas como como prueba espuria y habrá dentro de los procesos, porque incluso los fiscales ahora están solicitando que la gente la indagatoria firme varias veces para hacer pruebas. Grafoscópicas verdad de. ¿De esos vos sabes que ya es el el imputado como como sujeto y ya como objeto, verdad? O más bien al reves

Orador 2

Claro, como objeto. Prender.

Orador 1

¿Sí, ajá, entonces? ¿Di básicamente esa prueba viene a ser ilegal, entonces la defensa y lo que hace es que inmediatamente deja, constan y hace manifestación y directamente de que eventualmente, si se va a utilizar esas firmas para realizar cualquier tipo de prueba gráfica, habría ahí una actividad procesal defectuosa, verdad? ¿Porque muy por debajo de las garantías mínimas que ordena, verdad lo que es la norma? Y la Constitución y demás. Entonces, básicamente yo creería que el el poder judicial, para poder verdaderamente abordar, tendría que establecer una conexión directa, más bien con las entidades bancarias o financieras que controlan los sistemas, para que eso sean los que les puedan brindar la información adecuada para poder rastrear a las personas verdaderamente que cometen los delitos, no a simple y sencillamente personas que se fueron instrumentalizadas u otros. O sujetos. Crearía Yo.

Orador 2

Claro. Bajo los casos que usted me mencionaba que llevó en su función de defensora. ¿Podríamos decir que hubo una falta de malicia de esas personas que fueron imputadas.

Orador 1

Sí, y en otras oportunidades también. Porque también recuerdo un caso de una muchacha que ella me comentaba que ella realmente nadie le contactó, dice ella. Que ella solo tenía una situación de necesidad. En ese momento no tenían trabajo y se encontró un montón de dinero en una cuenta y

la. Y la gastó, digamos. Ella sabe que la gastó y nunca nadie se la pidió y ella la gastó. ¿Entonces este son poblaciones en condiciones de vulnerabilidad, ya sea por confianza o por una situación de necesidad económica, verdad, que se vieron en la consumación del delito como tal, pero no, nunca tuve contacto con alguien que es usual. ¿O sea, no, yo sé que si bien es cierto, hay perfiles, verdad? ¿No? ¿Bueno, no existe perfiles, pero uno va viendo como ciertos comportamientos con las personas a las que atienden y en estos casos eran personas que no eran como con antecedentes, verdad de la misma actividad delictiva, sino que básicamente lo que yo percibí como tal de partir de lo que la gente le dice a uno, verdad? Era pura inocencia.

Orador 2

Claro. Licenciado, le agradezco mucho su tiempo la información que me ha brindado hacer de mucha ayuda para mi tesis.

Orador 1

Muchísimo gusto, espero, verdad que le pueda servir un poquito por lo menos.

Orador 2

Claro que. Muchas gracias.

Orador 1

Con gusto

Entrevista a Fiscal de la sección de cibercrimen del MP

Archivo de audio

Audio entrevista Fiscal Cibercrimen

Orador 1: Jhonny Rojas

Orador 2: Fiscal de la sección de cibercrimen

Transcripción

Orador 1

Bueno, Buenos días.

Orador 2

Buenos días

Orador 1

Mi nombre es Johnny Rojas, estudiante de la UIA, maestría en Derecho Penal. La presente en una entrevista a profundidad a funcionarios que trabajan en el Poder Judicial. Mi tema de la tesis es retos de la individualización de la persona autora del delito de estafa informática, por lo cual licenciado, le agradezco mucho su participación y anuencia colaborarme

Orador 2

Con mucho gusto

Orador 1

Gracias voy a generar una serie de preguntas guías para encausar una conversación, fluía dentro de la entrevista, licenciado, ¿Cuál es su puesto dentro del Poder Judicial?

Orador 2

Fiscal coordinador de la unidad de cibercrimen del Ministerio Público.

Orador 1

¿Perfecto, entonces podemos pensar que tiene experiencia en lo que son delitos de estafa informática?

Orador 2

Sí, en efecto, tengo más de 13 años laboral como fiscal y concretamente de trabajar en esta unidad, específicamente 4 años y fundiendo como Jefatura año y cuatro meses.

Orador 1

Gracias. ¿Qué tan común es atender delitos de estafa informática, licenciado?

Orador 2

Es bastante común. De hecho, el delito estafa informática, concretamente al día de hoy, representa el cuarto delito de mayor ingreso en la totalidad del circulante del Ministerio público, es decir, no solamente de la unidad especializada, la unidad de cibercrimen, sino que de todas las fiscalías de todo El País.

Orador 1

¿Es un delito que ha venido un aumento de de cómo qué año calculas vos que pueda venir en aumento?

Orador 2

A partir del año 2018 y específicamente, los números vienen en incremento para el año 2018, concretamente la cifra aproximada de ingreso era de 3000 y resto de denuncias y el año anterior 2023, se cerró específicamente con más de 13000 denuncias de estafa informática. Eso representa un crecimiento aproximadamente en cuanto mayor 450% del fenómeno en cuanto a ingreso de denuncias ante el Ministerio.

Orador 1

Son muchos delitos informativos, muy exponencial la cifra.

Orador 2

¿Es bastante concretamente el fortalecimiento o la incremento en esa suma? Nosotros hemos podido el estudio que hacemos de métrica. Podemos determinar que este crecimiento se encuentra bastante ligado con el tema de la pandemia finales del año 2019 o del año 2020. Y esto tiene un sentido lógico. Y es que con la pandemia en virtud de las medidas, se otorgaron por parte del Ejecutivo y una de ellas era específicamente el hecho de que las personas no podían salir de las casas. Esto implicó, tenían más acercamiento con medios electrónicos y evidentemente los bancos fortalecieron sus plataformas electrónicas facilitando el ingreso de los usuarios y evidentemente los delincuentes. Vieron esto como una plataforma delictiva, como una oportunidad delictiva. Y fueron perfeccionando sus técnicas, principalmente de ingeniería social. Tendientes a poder dar convencimiento a las personas ofendidas de que se trataba de algún contacto de una entidad gubernamental, de un contacto de una entidad financiera para finalmente poder llevar a cabo estafas informáticas.

Orador 1

Sí, claro, don Esteban, y dentro de esta ingeniería social. ¿Como medio, cuál es el medio que más se utilizó el delincuente para la estafa informática? ¿Entiendes llamadas telefónicas, mensajes o páginas de Internet?

Orador 2

OK, el de mayor alta incidencia según lo que hemos podido obtener. Por parte de los compañeros del organismo de investigación judicial, anteriormente la sección de fraudes, recientemente, ahora justamente este año la sección especializada con fraude informático es que la modalidad de estafa informática mediante ingeniería social de mayor a alta incidencia es específicamente la de vishing son las llamadas telefonicas. Lo que sucede es que sí, el el grueso es de esa modalidad de llamada de vishing, pero generalmente se acompañan de otras técnicas, como específicamente también en campaña de Fishing que se mezclan a su vez. Entonces puede iniciar, por ejemplo, con una llamada telefónica y a su vez remiten a la persona ofendida a un enlace malicioso que de previo lo fue remitido por correo electrónico o eventualmente también en casos no, no, no tan altos. Y dice también con la llamada telefónica. Y posteriormente se le hace llegar a la persona un correo malicioso, un. Maliciosos y un smiching, ya sea por SMS o eventualmente por medio de plataformas de comunicación, como lo sería Whatsapp, que es la más habitual.

Orador 1

Claro, también dentro de la ingeniería social, el de la llamada telefónica. Según el análisis de jurisprudencia que he realizado, la mayoría de las víctimas facilitan esos datos en por llamada telefónica. ¿Verdad? Y hay tercera persona que manipula el sistema. Por ende, bajo ese análisis se puede deducir de ustedes como expertos de que el delito estafa informática se realiza en coautoría o de una forma individual.

Orador 2

Claro, innegablemente y De hecho, esa es la posición del Ministerio público a la hora de enfrentar esos procesos en etapa de debate, Y es que nos enfrentamos a delincuencia organizada como tal, son estructuras criminales en donde al menos nosotros hemos podido individualizar al menos 4 personas que conforman esta estructura general, desde una persona que se encarga de generar la llamada telefónica la inicial, ya sea indicando que se trata de un contacto bancario, indicando que se trata de un contacto gubernamental o eventualmente inclusive también de que es una falso comprador de algún artículo que tiene la persona ofendida publicada en alguna página. Posteriormente, generalmente se enlaza la llamada tercera persona a una segunda persona en este caso que va a fungir y cuando se trata de llamadas, la intención de generar un artículo de compra y venta, o un falso funcionario bancario o evidentemente otro funcionario bancario adicional al primero que llamó y además, evidentemente, como se acompaña en estas llamadas de ringtons de las entidades financieras, de correos electrónicos que simulan ser una determinada entidad financiera? Podríamos hablar de otro tercer sujeto con algún conocimiento básico de programación al menos, o conocimientos informáticos con intención de poder generar esas estas cuestiones que son meramente técnicas y además también tenemos la figura de El cuenta destino, que es la persona a quien finalmente se le remiten los fondos. Que son sustraídos ilícitamente de la cuenta bancaria de la persona ofendida una vez que se obtienen sus datos sensibles y que se manipula el sistema informático. Entonces al menos tenemos cuatro personas y podemos sumarle también en otras dinámicas que hemos visto cuando estos cuentas destinos, ellos venden sus cuentas y sus tarjetas, evidentemente el acceso a sus cuentas bancarias a una otra persona. Adicional que se las compran con sumas que van desde los 10000 corones en adelante y ya teniendo varias tarjetas se traslada hasta un cajero automático al realizar retiros masivos y con esas tarjetas y generalmente a esta a esta persona se le da la nomenclatura de Reclutador y entonces por eso es que podemos definir fácilmente de que sí estamos en presencia de coautoría y específicamente de estructuras organizadas.

Orador 1

¿una vez que se da el delito estafa informática qué procedimiento tiene el Ministerio público o existe un procedimiento como tal?

Orador 2

Sí, en efecto, Ministerio Público tiene directrices administrativas internas para poder enfrentar y dar trámite específico al delito de estafa informática. El procedimiento es primero esperar que después de que se interpone la denuncia por parte de la persona ofendida que lo hace ante el organismo de investigación judicial, toda vez de que lo hace con la persona ignorada que una vez inicie la investigación, se recibe un primer informe preliminar en el cual se hace referencia acerca de El relato de la persona ofendida, a la dinámicas, específicamente de circunstancias, de modo, tiempo y lugar de los hechos, el perjuicio ocasionado a la persona ofendida y detalles en cuanto a la cuenta afectada y la cuenta destino, esto ya una vez recibido por parte del Ministerio público, el siguiente paso es poder gestionar una solicitud de levantamiento de secreto bancario que se dirige al juez competente, quien conocerá la misma. En el en el caso de ser positivo, ordenará específicamente el el levantamiento del secreto bancario. Con ello se redirecciona nuevamente a la Policía Judicial, con intención entonces de que proceda a generar respectiva notificación a la determinada entidad financiera de la persona cuenta destino, con el fin de poder obtener esta data protegida por secreto bancario de la cuenta de la persona encantada y poder terminar situaciones tan relevantes como es la habitualidad de la cuenta, que era lo normal y que ocurriera que ocurriera en esa cuenta. ¿Cuáles eran los débitos y créditos que tenían anteriores? Realmente se solicita 6 meses antes y para poder ver esta dinámica, estos movimientos que tenía y un mes posterior a la fecha de los hechos que dan entras entidades financieras desde su proceder administrativo han bloqueado esa cuenta. Entonces ese mes antes es únicamente en caso de que nos lo hayan bloqueado, generalmente nos vamos a quedar hasta la fecha de los hechos y teniendo esta información es cuando ya Ministerio Público podría decirse que puede tomar decisiones de carácter investigativo. Como lo sería eventualmente poder generar orden a la Policía Judicial y con la intención de secuestrar los dispositivos electrónicos de la próxima cuenta de destino o verificar además, si porta consigo, la tarjeta ligada a la cuenta vinculada a los hechos, poder definir eventualmente un en casos relevantes, por ejemplo, activaciones de Radio bases, llamadas entrantes y salientes para fechas cercanas a los hechos y poder entonces seguir escalando. En esa estructura criminal que como dijo que es innegable que así ocurre, lamentablemente esto no es factible, en todos los casos estamos hablando de estructuras criminales, cometen delitos de cibercrimen y si bien en cuenta destino podríamos decir es el eslabón más débil de esta cadena. Cierto es que el resto de las personas que lo componen y que tienen posiciones de liderazgo, pensemos y hablemos

de las personas, las personas que hacen las llamadas inicialmente o de esos programadores o informáticos que generan la plataforma fáctica para poderlo realizar. Evidentemente saben lo que hacen y entonces se protegen con también técnicas informáticas que muchas veces impiden llegar a identificar. Y entonces que esto representa un riesgo, un reto más bien para el Ministerio público y es el poder procesar únicamente al cuenta destino. Ese es el el grueso de los casos. Evidentemente, en asuntos ya con declaratoria de criminalidad organizada como ley de crimen organizado, ofrece otro tipo de posibilidades probatorias, como lo sería la intervención de las comunicaciones, por ejemplo. ¿Se pueden hacer uso de otras técnicas de investigación? Y es más factible poder escalar en esa estructura, pudiendo determinar esas figuras de liderazgo y generar finalmente y es el interés principal en la atención de este tipo de casos de criminalidad organizada, una diligencia de allanamiento en donde en muchas oportunidades obtenemos prueba directa, prueba material y prueba, en este caso digital, que vincula a las personas encantadas con la realización de estos delitos de estafa informática por parte de estructuras criminales.

Orador 1

Gracias, ahora que me hablaba del crimen organizado. Se da la solicitud para que se declare crimen organizado en ese tipo de estafas.

Orador 2

Sí, en efecto, como yo me decía inicialmente, quien realizan investigación y quienes brinda a nosotros esos insumos de investigación es la Policía Judicial, entonces ellos de previo ya por ejemplo, identificado causas con factores comunes. Pensemos este que no solamente se hicieron llamadas, sino que se le emitieron correos electrónicos. Y resulta que si hay un correo electrónico que es un factor común en otras estafas informáticas, es decir, a diferentes ofendidos. ¿Es factible poder deteriorar entonces el llamado factor individualizante, un factor común. Entonces se trabajan en bloque y con eso entonces podríamos eventualmente esperar información a ese proveedor de ese servicio de correo electrónico y poderle solicitar información de datos de abonado identificado esto, podríamos evidentemente escalar en esa organización, tener un informe preliminar y solicitar ante control jurisdiccional la declaratoria de crimen organizado y De hecho existen investigaciones

en curso se han realizado también otras investigaciones. Y con esta técnica que ha permitido posteriormente realizar la intervención de las comunicaciones y finalmente, diligencias de allanamiento.

Orador 1

¿Claro, y qué tan efectivo ha sido para identificar, aparte de la persona que hace el retiro en el cajero automático o en la ventanilla del Banco, poder alcanzar a otros imputados?

Orador 2

No, no ha sido tan factible. Únicamente tenemos experiencia en pocos casos, casos sí exitosos. Y esto precisamente por las técnicas informáticas que realizan las personas más elevadas de la estructura criminal. Por ejemplo, pensemos de que detectamos un correo electrónico y que es factor común a diferentes estafas informáticas. Cuando nosotros gestionamos esta solicitud de datos de abonado a ese proveedor de servicio del proveedor electrónico no necesariamente va a colaborar primero con la con la investigación. Hay determinados proveedores de servicio que no no brindan información o que por sus condiciones de privacidad concreta del correo, pensemos el pronto en gmail por ejemplo, no brindan información. Pensemos de que sí nos va a dar información. Esto no implica que la misma sea fidedigna sea cierta, porque bien estos datos de abonados podrían ser falsos y si bien nos otorgan información por ejemplo muchas veces de direcciones IP, resulta que ante la existencia de técnicas informáticas para desviar esta esta atención, los delincuentes podrían utilizar, por ejemplo, VPNS podrían utilizar proxys. Podrían utilizar la red Tor y máquinas virtuales, es decir, hay infinidad de posibilidades. Y que muchas veces nos lleva a un callejón sin salida, nos desgastamos es grande en esta información para finalmente darnos cuenta de que el el la persona encartada que generó ese correo electrónico con el cual se le emitiera el correo maliciosos, lo hizo por ejemplo mediante un servicio de VPNY, y al solicitar la información a ese servicio de VPN o no tienes Datos de abonado. O resulta que es un servidor que a su vez le aloja información a otro servicio VPN entonces te presenta dificultad? En efecto, el tema de obtener evidencia digital, que a final de cuentas es lo que se requiere para la demostración o vinculación del resto de estructura criminal distinta a la persona, cuenta destino.

Orador 1

Claro. Puedo preguntar que si existe otro, retó don licenciado, que es que si logran identificar dueño del correo de dirección IP exacta, bajo la premisa que el Derecho penal es personalismo. ¿Como o el reto es cómo saber que el dueño de la IP fue el que realizó el delito?

Orador 2

Sí, en efecto, esto me presentaría también otro reto, evidentemente, y hay una cuestión que es fundamental al obtener, por ejemplo, pensemos que una IP positiva y un correo electrónico también positivo, que nos da información cierta, pensemos de una persona que fue la la que como abonado generó este correo, esto es información plana, es totalmente plana y tiene que acompañarse con técnicas de investigación de Campo, entonces los compañeros de OIJ tendrán que ir a verificar trasladándose al sitio a verificar esta información, verificar si es la persona que hace uso, no este correo. Ya y es y es meramente un indicio, es un indicio que tiene que acompañarse a su vez de otros indicios. Y entonces, por ejemplo, la investigación mediante técnicas o SIM es muy relevante, porque entonces podríamos o se podría introducir ese correo electrónico o ese número del teléfono que vinculó a la persona abonada a la hora de generar ese correo en otras redes abiertas, con intención de poder definir de que, en efecto, esta persona le venía dando un uso habitual a ese correo determinado, lo cierto es que eso es es mera prueba y de carácter indiciario, y que entonces este será finalmente o un juez quien le tenga que dar el valor probatorio específico a esta a estos hallazgos de carácter inicial.

Orador 1

Claro, en primera instancia, cuando la víctima va a denunciar, hay información importante que el investigador necesita recabar para poder tratar de identificar al delincuente.

Orador 2

Si de hecho claro, Y es otro de los retos también aquí aquí vamos a hablar bastante de retos, que es el hecho de que la información que el ofendido generalmente viene, nos brinda a nosotros. Es información también muy escueta. Es únicamente el detalle de, evidentemente, la llamada que recibió cuando es por llamada y los movimientos que se realizaron cuando es directamente por viching y los ofendidos, que generalmente son personas comunes, como todos los demás, ellos no tienen conocimiento técnico, no son especialistas en ciberseguridad, no son abogados, inclusive tenemos también personas en esa condición de ofendidos y esto no implica entonces per se de que tengan que tener un conocimiento tan avanzado? ¿Por qué lo Digo, porque esas campañas de vitching se han ido perfeccionando bastante y al punto de que los ofendidos ni siquiera reconocen el punto de compromiso, entonces hemos podido determinar, por ejemplo, campañas de viching, que lo que hace es una remisión. Haciéndose pasar por Un proveedor de servicio de pensemos este, por ejemplo. Por ejemplo, de televisión, como sería Netflix, en donde le indican a la persona ofendida de que su tarjeta bancaria ligada a su cuenta de Netflix ya venció o que tiene que actualizar la información. El ofendido Ni siquiera reconoce ese punto como compromiso. Posiblemente se hizo bastante tiempo. Tiempo atrás y cuando ya las personas atrás de esta de esta remisión de ese correo de Fiching se han impuesto los datos sensibles de acceso a la cuenta bancaria de la persona ofendida, es cuando ya ellos han realizado el movimiento y la persona ofendida ni siquiera recuerda el haber brindado en algún momento ningún detalle de información, entonces esto esto pues resulta relevante. Y entonces, de ahí en adelante resultaría importante para los compañeros del organismo de investigación judicial precisamente, poder generar una ampliación de esa denuncia para poder tratar de ubicar ese punto de compromiso, tratar de refrescar a la memoria de la persona ofendida, eventualmente aplicar técnicas también ya en conjunto con la sección especializada contra el cibercrimen, para que si el si hubo una remisión de un correo, se puede realizar el respaldo él mismo, si hubo el acceso a un enlace malicioso y poder también respaldar adecuadamente ese enlace como tal y obtener algún tipo de información. Y como reto principal, además, es el hecho de que ahí data que el propio ofendido podría facilitar. En el tanto las entidades financieras no tuvieran una mala apreciación de El secreto bancario. ¿Y esto por qué? Porque resulta que de todos estos movimientos que se realizan en una plataforma informática. Dentro de la cuenta bancaria ligada a la persona ofendidas queda rastro también electrónico y son precisamente las bitácoras web. ¿Y estas bitácoras web no son propias del secreto bancario porque no haga de cuentas, por ejemplo, el tema de movimientos de saltos, de créditos, de débito, de movimientos bancarios como

tal es mera data informática y resulta relevante porque entonces nos va a otorgar a nosotros también que a los compañeros investigadores información, por ejemplo, de cuándo es que se da el acceso, en qué momento, desde qué dirección IP, de qué dispositivo se utilizó? De igual forma, si se hizo alguna algún cambio de contraseña también va a conservar esta misma información, el tipo de dispositivo la IP también. Y en igual sentido, cuando se remiten las transacciones al obtener esta data técnica de bitácora web. Eso podríamos compararlo, por ejemplo, con la información que obtengamos del correo electrónico ligado el enlace malicioso de la generación, por ejemplo, de una página. Pensemos que un dominio y al consultarle al proveedor de servicio de ese dominio quién fue la persona que creó el dominio como tal, nos va a brindar también un correo electrónico y podríamos seguir ese mismo ejercicio de ir comparando información técnica hasta eventualmente tener indicios suficientes que nos puedan ligar. A otra eventual persona, Lo que pasa es que hemos tenido dificultad con esto, con los bancos. No son todos los que le facilitan esta información a la persona ofendida. Ante esto, nosotros hemos realizado reuniones con ellos haciéndole ver esta cuestión y hemos llegado inclusive también al punto de poder colaborar o trabajar de forma conjunta con la Agencia de Protección de Datos de los habitantes, quienes nos facilitaron un modelo que tienen ellos De hecho, su página web para que las personas ofendidas directamente le soliciten esa data personal, esa data que les pertenece directamente a ellos, a las entidades financieras que tiene un tiempo de respuesta específico. Y entonces, hecho esto, generalmente los bancos les dan la información que para nosotros resulta mucho provecho.

Orador 1

Claro. En el caso del vichín o la llamada telefónica. Si la persona víctima indica sí, “yo di los datos pensé que era el funcionario, o sea, me engañaron, yo los di de buena fe”. ¿Hay un trato diferenciado por parte del Ministerio Público en el sentido de que usted dio los datos? No se los robaron por medio de una página o malware. Usted los editó erróneamente. ¿Cuál es la posición en caso de las llamadas? Y la víctima si da el dato, si yo di la cuenta, yo di el usuario.

Orador 2

No, no lo hay en virtud de que la persona es ofendida, la persona es ofendida y evidentemente no le es reprochable dentro del proceso penal costarricense de ninguna forma en, de cierta manera colaborar para la realización del hecho. ¿Y esto precisamente por qué? Porque los delincuentes, como les decía, a partir del año 2020, después del tema de la pandemia, ellos se han ido perfeccionando esas técnicas y entonces no es esperable. No es este ni siquiera una cuestión lógica el hecho de que las personas ofendidas. Obligatoriamente, tengan la necesidad o tengan La exigencia de no brindar data. Esto esto va a seguir ocurriendo porque los delincuentes van a seguir buscando formas. ¿Lo que a mi criterio sí es relevante y sí resulta este una cuestión, si se quiere también de responsabilidad, es el hecho de que las personas ofendidas, son humanos, van a seguir cometiendo errores? Van a seguir siendo engañadas eventualmente, pero las entidades financieras tienen responsabilidad, puesto de que ellos administran fondos privados. Son fondos que son de las personas ofendidas. ¿Y qué las entidades financieras tienen pues ganancias a la hora de administrar estos fondos? Y ellos bien podrían detener. Empecemos en el Banco o en la entidad financiera de las personas ofendida. Ellos podrían realizar un ejercicio de Habitualidad en esa misma cuenta. Y esa habitualidad, evidentemente, podría realizarse mediante factor humano o bien el mejor de los casos con inteligencia artificial, determinar que es lo habitual en esa cuenta de esa persona ofendida. Pensemos de que se trata de un adulto mayor o pensemos de que es una persona empresaria que ha tenido siempre una suma considerable de altos millones de colones no es normal. Y el hecho de que esas personas, una persona empresaria, un adulto mayor. Que remitan en una sola transferencia y un movimiento hacia una cuenta con la que nunca antes ha tenido ningún tipo de relación previa. Esto pues no es lógico, y mucho menos tampoco cuando esta suma de dinero se traslada a hacia los bancos o las entidades receptoras que representan los cuenta destinos y las personas. Cuenta destinos, como cualquier otra persona normal, genera una cuenta bancaria del tipo que sea, tiene que brindar políticas, que si hay, sí políticas conozca a su cliente. Entonces tampoco resulta lógico el hecho de que una persona que dice mira que va a recibir fondos, productos de trabajo y entonces va a ser salario y pensemos que ese salario es de 500000 colones, nada hace una persona de estas recibiendo sumas millonarias esto es totalmente ilógico y De igual forma, si se realizara un monitoreo específico en ambos sentidos, tanto en Banco de la persona ofendida o en Banco de la persona encantada, ni siquiera se podría llevar a cabo el delito. Eso serían acciones preventivas oportunas de la realidad es otra, la realidad es que lamentablemente no es así, no funciona de esta forma. Y lo digo con total certeza, porque los números hablan por si mismos son

más de 13000 denuncias que se siguen recibiendo por parte del Ministerio público y evidencia que el trabajo preventivo no está siendo el adecuado. Devolviéndome con el tema de la del eventual reproche que se puede hacer a la persona ofendida al Ministerio Público, es muy claro en el hecho de que esta cuestión de que los ofendidos van a seguir y lamentablemente cayendo. Y ante eso entonces se ha decidido, ante la creación de la unidad de cibercrimen, el fortalecer, pese que no nos corresponde, puesto que nuestras labores es meramente represiva, el poder trabajar en carácter preventivo. En conjunto con la oficina de prensa Institucional, oficina de prensa, también de organismo de Investigación judicial y en cada oportunidad que tenemos de que un medio de comunicación solicita una campaña o solicita una entrevista, acudimos lo antes posible para precisamente ir realizando información y dando a las personas ofendidas y dentro de lo posible, ir disminuyendo esta cifra de personas que son afectadas con este tipo de delincuencia

Orador 1

¿En el caso de la estafa, cuando saquean la cuenta del Banco? El Banco colabora con la obtención de prueba. ¿Y qué posesión tiene el Banco si lo conoce usted ante la víctima, que es defraudada?

Orador 2

OK el Banco de inicio no va a colaborar con la investigación. En el tanto no exista de por medio un secreto o un levantamiento, un secreto bancario. previendo esa posición de nuestra parte, se ha generado desde el inicio propio desde que asumi el cargo como encargado de la unidad de cibercrimen. Dos documentos pendientes a que pese a esta falta de interés de colaborar con las entidades financieras, entonces exista algún tipo de exigencia y es una orden de preservación de data informática, que a nosotros es lo que nos va a servir. Entonces le solicitamos a las entidades financieras vinculadas a la cuenta del cuenta destino. Que presenten data, como específicamente las bitácoras web de esa cuenta destino y además los vídeos de seguridad y evidentemente también el tema del resguardo del baucher en caso de que sea efectivo mediante cajero físico, porque es data muy relevante que nos a Nosotros a servir finalmente obtenido ya levantamiento ese efecto bancario para poder individualizar a la persona que hace el retiro de los fondos, cajero automático o evidentemente en cajero físico y además también otro documento que es el que les hablaba al

hablaba anteriormente, que se le entrega a la persona ofendida con la intención de que él directamente vaya acuda a la entidad financiera que le representa para pedir también su bitácora web. Poder obtener esta información. Respecto a la última consulta de cuál es la posición de las entidades financieras hacia con los ofendidos, en la experiencia de lo que nosotros hemos podido recibir y una vez que pudimos levantamiento de secreto bancario y nos aportan también la investigación administrativa. Investigación interna es que ante el reclamo de la pensión ofendida, si la pensión ofendida recibió una llamada y facilitó información o accedió a un enlace malicioso, lamentablemente las entidades financieras no se hacen cargo de los montos sustraídos. Y los objetivos deben de acudir a otras vías, de la experiencia que tenemos también de la del seguimiento que hemos hecho con las personas ofendidas. Hemos podido ver que hubo un gran número de ellos. Dichosamente ha podido acudir a la sede del contencioso administrativo, han iniciado procesos contencioso administrativos en contra de entidades financieras y en algunas oportunidades han logrado obtener sentencia favorable a sus intereses y sea condenado a la entidad financiera por parte del Tribunal contencioso a poder resarcir los daños ocasionados a la persona ofendida.

Orador 1

Gracias. Licenciado, considera usted que se logra llevar al autor intelectual de la estafa informática al proceso penal.

Orador 2

No, se sigue en trámite, se sigue llevando en la mayoría de los procesos y el fuerte de los casos se sigue procesando al cuenta destino. Justamente en la Fiscalía General tienen la intención, ante la nueva creación de una unidad específica en el OIJ, que es la sección contra el fraude informático que inició funciones el pasado mes de febrero de este año, es poder fortalecer la el rumbo investigativo tendiente a poder seguir escalando. Y poder individualizar al autor intelectual de esta de esta delincuencia que en casos ajenos o casos diferentes a criminalidad organizada únicamente se procesa el contra destino.

Orador 1

¿Claro, cuál es la posición de los imputados que sí se logran llevar el proceso penal en brindar información que permitan identificar al posible autor intelectual?

Orador 2

Es muy baja esta esta posibilidad y en virtud de que ellos son procesados como personas imputadas específicamente por coautoría, muchos de ellos lo que hacen es o abstenerse a declarar es su derecho, específicamente, obviamente brindar una declaración como también es su derecho y es una declaración generalmente tendiente buscar impunidad. Ellos lo que indican es que facilitaron esa cuenta bancaria que desconocían que iba a ser utilizada, por ejemplo para una estafa informática, que fue un favor que le pidió a una persona allegada o un familiar o algún vecino, mas no aportan ningún tipo de prueba pese a esas declaraciones, el Ministerio público de forma objetiva. Si no logra acreditarla, si no logra acreditar el dicho de la persona encantada, lo que va a gestionar es en llevar del proceso a juicio y Buscar evidentemente una sentencia de carácter condenatorio, esto porque la participación que tiene ese cuenta destino, en que haya sido de él quien le tiró dinero en cuestión, es igual que la de cualquier otra persona que formó parte de esa estructura criminal, precisamente porque estamos ante coautoría, en donde se ha hecho una decisión de diferenciar esta coautoría. Y evidentemente, terminar más bien una complicidad ha sido en el asunto de las personas que han vendido Su cuenta bancaria y es otra persona que evidentemente no se puede individualizar o que eventualmente sí fue individualizada quien hace los retiros de los fondos y a estas personas entonces se les ofrece un criterio de oportunidad para que precisamente brinden algún tipo de data relevante en la investigación y poder llegar y a donde se llega generalmente es a la persona que funge como reclutador que fue la persona que se les acercó a ellos y les pidió la venta de la tarjeta como tal, no, aún así no es posible llegar, evidentemente el autor intelectual, evidentemente, a quienes ostentan puestos de de de Jefatura o de encargado dentro de la estructura criminal.

Orador 1

¿Claro, cuáles considera usted licenciado, que son los principales obstáculos para identificar al ciberdelincuente?

Orador 2

Yo creería que precisamente primero, el más importante es la falta de colaboración de entidades financieras, la falta de interés en resguardar data relevante para para este tipo de acreditación de estos hechos y además también el hecho de que estamos hablando de cibercrimen puro y duro, que los delincuentes que lo realizan en esas estructuras de altos mandos son personas como indicada, saben lo que hacen, que van a utilizar en medios tecnológicos tendientes a que no se han individualizado. Y esto representa el principal reto para poder identificar concretamente, pues a ellos.

Orador 1

La misma tecnología, los amparo.

Orador 2

Exacto

Orador 1

¿Se están tomando algunas medidas para superar esos desafíos por parte del Poder Judicial?

Orador 2

Sí, en efecto, Ministerio Público es hecho el principal ente que ha impulsado la rectificación del segundo Protocolo adicional del Convenio de Budapest, el que otorga mayores herramientas de Cooperación Internacional de obtención de medios de evidencia digital, también directamente a las autoridades. Y se está trabajando en conjunto con la Cancillería y la presentación del proyecto de ley, con la intención de que él mismo este este segundo protocolo adicional se convierta en ley de la República. Esto permitiría, por ejemplo, que hacemos que estamos hablando de data, que se

encuentra almacenada en otro país, que también forma parte del Convenio Budapest y pensemos que es un proveedor de servicio que anteriormente no daba información y que pedía que se tramitaran ante la vía normal de asistencia penal internacional, que es bastante lenta. Esto permitiría entonces a las autoridades ahora tanto a policía como al Ministerio Público, poder realizar gestiones directamente y estamos entonces tratando de encaminar esto a ir generando mayor robustez, en cuanto a legislación nacional y que permita entonces pues obtener mayores medios para la procuración de evidencia digital. E igual sentido se ha tenido también acercamiento con fracciones legislativas con intención de poder también presentar proyectos de ley pendientes o dar recomendaciones a proyectos de ley que De hecho ya fueron presentados y de acuerpo, concretamente los de la unidad social cristiana. El diputado Leslie Borges, que presentó al menos 4 proyectos de ley por recomendaciones del Ministerio público que precisamente van a otorgar mayores facultades a la hora de investigar, concretamente el delito de estafa informática debido al crecimiento que ha tenido.

Orador 1

Claro, esperemos que sí. Existen herramientas tecnológicas. Que no se estén usando que se podrían usar para identificar al delincuente ciberdelincuente.

Orador 2

Sí, en efecto, y yo creo que el el es el tema enboga, que es la inteligencia artificial. Con esto sí nos estamos quedando cortos, no solamente las autoridades de investigación, sino también las propias entidades financieras, que a final de cuentas es donde nacen, donde ocurre este fenómeno delictivo. Si ellos utilizaran inteligencia artificial y pensemos que machine Learning, por ejemplo, dentro de sus sistemas serían más procedentes el hecho de prevenir tal la delincuencia y en caso de que se busque por parte de los delincuentes, que esto va a ocurrir siempre. Puesto que son a carrera armamentista una forma de cómo vulnerarlo, de cómo superarlo, eventualmente estos mismos sistemas robustos de ingeniería social serían más factibles de captar información, de guardar data y que a su vez, el Ministerio público podría obtenerla posteriormente, una vez que se se se recabe la misma por parte de El organismo de investigación judicial. Y en igual sentido, sería poco sería

propicio que tanto la Policía Judicial como el Ministerio público también encontramos con sistemas de inteligencia artificial. Y que no sea un factor humano quien tenga que realizar la previsión para poder vincular factores comunes en las investigaciones, sino que si se alimenta un sistema, el mismo sistema podría encontrar esos factores comunes y evidentemente podría ir generando investigaciones cada vez más grandes y que permitirían entonces acudir a esa vía, que es más más oportuna de la gestión de criminalidad organizada.

Orador 1

¿Claro, en cuanto a la Cooperación Internacional, licenciado, considera usted que hay? Medidas en cuanto. ¿Qué se puede mejorar con la Cooperación Internacional?

Orador 2

En Cooperación Internacional yo creo que lo más importante es el tiempo, si nos vamos a Cooperación Internacional tradicional para que se transmitan mediante, mediante o promedio de la oficina específica de la Water, y ésta lleva bastante tiempo, y entonces este tiene que tramitarse y pensemos que comparta juzgatoria o tiene que tramitarse ante el control jurisdiccional. Y esto lleva, pues bastante tiempo. Dichosamente el Convenio Budapest y lo que pasa es que se aplican a menor cantidad de las veces. Es un medio oportuno para precisamente poder obtener evidencia de índole digital o cooperación en asuntos de cibercrimen. Y al ser estafas informáticas, un delito de cibercrimen es precisamente medio oportuna que se puede utilizar para captar información. Nosotros en las investigaciones que hemos realizado, concretamente de estafas informáticas, han sido muy pocas las que hemos requerido asistencia penal internacional, en virtud de que. Las estructuras criminales que operan en nuestro país son meramente domésticas. operan acá, si hemos tenido pues alguna experiencia de cooperación con Perú y uno de los problemas también que hemos visto son estructuras domésticas que emigran a Nicaragua y con Nicaragua, tenemos un problema este pues de comunicación, lamentablemente ellos no brindan la mayor cantidad de información que se quisiera y entonces las investigaciones pues no, no resultan tan relevantes. Y es un reto que creo que tenemos que actualmente y que no depende directamente, pues del Ministerio público, ni tampoco del Poder Judicial, sino que es una cuestión meramente. Si se quiere diplomática, tal vez

y que en el mediano plazo, yo particularmente, no creo que se vaya a solventar ese reto, al menos con Nicaragua.

Orador 1

¿Entiendo, claro, licenciado, alguna recomendación general que considere usted que podría funcionar para la identificación del ciberdelincuente dentro de su experiencia?

Orador 2

Yo creo que es un trabajo en conjunto y en ir asociando a más sectores involucrados, mucho de esta de esta delincuencia. En su estrato bajo, en sus coautores, que se dedican no a funciones específicamente de Jefatura de altos mandos. Son personas muchas veces que se encuentran, por ejemplo, dentro de centros penales. Entonces una recomendación relevante es, por ejemplo, poder trabajar y que De hecho se hace así, pero tienen que fortalecer. El trabajo conjunto con las autoridades penitenciarias. ¿Ir generando también porque por medio existe un tema de corrupción, esos teléfonos y esos dispositivos ingresan a los centros penales? Lamentablemente por una cuestión pues de corrupción, entiendo que recientemente y desconozco qué fracción legislativa lo ha presentado, pero hay un proyecto de ley tendiente a poder generar un nuevo tipo penal. En contra de las personas que ingresan dispositivos telefónicos a los centros penales, independientemente si es o No es un oficial o si es una persona particular. Evidentemente entiendo, tiene un agravante en tanto se trata de un funcionario público o de una persona en condición de abogado visitando a un a un privado de libertad. Y creo que es una pregunta oportuna y porque como digo mucho de esta de esta cuestión, lamentablemente ocurre por Ahí y esto necesariamente nos vincula también al papel necesario que tienen que llevar los proveedores de servicios de telefonía y de Internet. Si bien se han colocado dispositivos que logran bloquearlas la señal celular, lo cierto es que los delincuentes ellos siguen buscando formas de cómo saltar estos bloqueos y se han dado cuenta de que dispositivos chips o sin de otros países, pues lleva algún tiempo que el sistema los logre identificar. Y ese tiempo muchas veces es de 15 o 30 minutos, que les permite a ellos, con esos 15 ó 30 minutos, poder realizar bastantes estafas informáticas durante ese corto tiempo. Totalmente. También deberían de tener alguna responsabilidad mayor los proveedores de servicios de telefonía,

ellos deberían de estar comprometidos con esta cuestión y. Ir adelante de las formas que buscan los delincuentes para poder saltar esos bloqueos.

Orador 1

¿Entonces, podría deducir que dentro de las cárceles se gestan más este tipo de delitos?

Orador 2

En efecto y De hecho, estructuras criminales relevantes que nosotros hemos venido trabajando, tenemos conocimiento de que siguen operando lamentablemente dentro de centros penales.

Orador 1

¿Claro, don licenciado, se me surge la pregunta, cambiaría en algo si en lugar de imputado? Lo presentaran como testigos, si es posible dentro del proceso penal a la persona que imputan como tal a la persona que retiró el dinero, por ejemplo.

Orador 2

Sí, lo lo que pasa es que con un tema de coautoría ante específicamente la participación activa por Codominio funcional que tiene cuenta de destino dentro del proceso. A mi criterio no sería factible el poderlo poderlo utilizar como testigo, lamentablemente lo indico, yo eso lo entiendo a perfección. Es el eslabón más débil de esta cadena. No obstante, actúa con dolo, actúa con conocimiento, con voluntad y por ende. Debe de existir un una respuesta procesal por parte del Ministerio público y es precisamente perseguirlos a ellos y eventualmente, ante las posibilidades, ante los retos que teníamos que ya habíamos hablado, el poder escalar dentro de la organización. Y entonces dentro de Mediano plazo y en virtud de la legislación que tenemos actualmente, simplemente pues no sería factible poderlos utilizar en condiciones testigos.

Orador 1

Claro, entiendo, licenciado, le agradezco mucho su tiempo.

Orador 2

Con todo gusto para que servirle

Entrevista Juez de etapa intermedia

Archivo de audio

Audio entrevista juez etapa intermedia Jordan.m4a

orador 1, Jhonny

Orador 2, Juez

Transcripción

Orador 1

¿Buenos días, licenciado, cómo le va?

Orador 2

Buenos días, licenciado, Buenos días, gracias a Dios.

Orador 1

Gracias bueno, me presento, Mi nombre es Johnny Rojas, estudiante de la UIA Maestría de Derecho Penal le agradezco mucho su colaboración para para con mi persona, con el tema de mi tesis, que es “retos de la individualización de la persona autora del delito de estafa informática”,

para lo cual el marco teórico propone, realizar entrevistas a funcionarios del Poder Judicial, para lo cual agradezco mucho que me colabore.

Orador 2

Con mucho gusto.

Orador 1

Licenciado don. ¿Licenciado, cuál es su puesto, el Poder Judicial?

Orador 2

Ok, actualmente yo me encuentro adscrito al Poder Judicial en la judicatura desde el año 2017 como juez penal. Actualmente me estoy desempeñando como juez penal en el juzgado penal en turno del segundo circuito judicial de Samos, en Goicochea

Orador 1

Perfecto, posee experiencia en delitos de estafa informática, licenciado.

Orador 2

Sí, claro que sí, bueno, como le indiqué anteriormente mi experiencia como juez, en el año 2017, particularmente estuve nombrado en el juzgado penal de San José cubriendo el licenciado Andrés Hernández y mi primera audiencia preliminar fue precisamente un delito de relacionado con ciber crimen en la cual desde ahí pues ya me aboqué a tener participación en ciertos juicios valorativos en lo que respecta a delitos informáticos.

Orador 1

¿Qué tan común es atender este tipo de delincuencia informática en nuestro país?

Orador 2

Fíjate que esto ha tenido un alto índice de incidencia a nivel criminológico, porque sabemos de qué el comportamiento de las personas es cambiante y a cómo cambian las personas cambian la delincuencia y pareciera que hace unos, podríamos decirlo de esta manera, hace unos 15 años atrás nunca se hablaba o no se hablaba de delitos informáticos o si se hablaba. Hablaba muy poco. Y esta tendencia tuvo un alto apogeo ya cuando entraron hacer utilizados en nuestra sociedad como lo eran las plataformas virtuales Whatsapp, Facebook, Instagram. Y estamos hablando que ya después del año 2010 hasta la fecha es cuando ya incluso en la actualidad, partiendo del año 2015 hasta la fecha, el alto índice de delincuencias alto, valga la redundancia, es está un tope máximo que incluso. Parte de la práctica judicial a estos solo se asombra, y no solamente que ya las estafas ya no se hacen a través de incluso a nivel de llamadas telefónicas, se hacen a través de mensajes de texto plataformas como Facebook, Instagram, ahora la implementación de los famosos simpe móvil y también se he tenido la oportunidad de de observar incluso en cómo se envían correos electrónicos donde ya la persona incluso no tiene necesidad de hablar con el con el con el la parte ofendida. Se remite un correo electrónico, la persona abre el correo, abre un link y les aparece, y automáticamente eso existe un programa donde le jala la información y ya se obtiene la base privada o la base íntima de la persona a la cual ya, pues se hace la extracción antijurídica patrimonial de la parte ofendida. Entonces vemos que eso no es algo de hace unos 20 o 30 años atrás, sino que es algo muy nuevo. Y esa novedad, pues trascendió a raíz de la nueva implementación de de plataformas virtuales, que pareciera que eso nos viene a dar una facilidad en la utilización o la utilidad de nuestro diario vivir, pero más bien lo que hace un arma fuerte para la delincuencia y así evidentemente a ultrajar a las víctimas y a ocasionar daños patrimoniales antijurídicos.

Orador 1

Claro, todos podríamos indicar que la estafa informática ha venido en aumento de su desde su experiencia.

Orador 2

¿Es correcto? Podemos decir que Yo Yo pienso que desde que yo tengo experiencia como juez, aproximadamente como el del año 2018 a la fecha, sí ha venido en el momento, pero exponencial. Y podemos y existen grupos etarios todavía más vulnerables, que ese es el Grupo por el cual busca la delincuencia para afectar y el cuál es el el el grupo etario vulnerable, las personas adultas mayores, que son las personas que evidentemente tienen una economía no fuerte, pero tiene cierto patrimonio, por qué? Porque las obras que están evidentemente ya gozando de de una pensión y no sé si será parte de las preguntas que me indicarán, pero me adelanto a contestar donde mi experiencia como juez, he tenido la oportunidad de incluso a nivel de crimen organizado, incluso con herramientas de investigación como lo es la intervención telefónica, donde policialmente se manejo. Donde ciertos funcionarios que incluso a nivel del Banco le vende a las organizaciones criminales a qué persona contactar, a qué persona ubicar, porque no lo hacen al azar y ese es un aspecto que se tiene que quedar muy claro en ese tipo de delincuencias, y lo digo con el mayor de los respetos, o sea el delincuente de de ese el el autor de ese tipo de delincuencias, no va buscar a al vecino que no tiene ni un 5 en La cuenta sino. ¿Sabe a quién buscar? ¿Por qué? Porque ya tiene de manera anticipada los datos de esa persona que sabe cómo se llama, a qué se dedica y cuáles son sus ingresos. ¿Por qué? Porque sabe que la afectación patrimonial va a ser. ¿Satisfactoria para los intereses del criminal, porque yo sé que esa persona tiene dinero en su cuenta y es por esa razón de que las personas en ese grupo etario vulnerable son las personas o adultos mayores que cuenta con una pensión o incluso he tenido conocimiento de personas, no tan mayores pero que tienen vulnerabilidad. ¿Por qué? Porque las mismas personas saben de que no tienen conocimiento en aspectos informáticos y saben ush es que se me llenó un virus en la cuenta porque me acaban de llamar, no, no, eso hay que hacerlo rápido. Entonces saben porque ellos saben a qué persona va a dirigirse, por lo cual, lastimosamente también nosotros dos cosas somos ignorantes en el aspecto informático. Y esa ignorancia incluso trasciende a nivel de prevención, cuando el organismo de investigación judicial, las entidades bancarias remiten información donde no ellos no han piden información por correo, que no caigamos en estafas, pero a veces o la persona o no se informa bien o no quiere tener información bajo algún tipo de prevención y eso es lo que Todavía. ¿Tiene un auge en aumento en que las personas sean víctimas de este tipo de delincuencia? YY lo voy a decir

con todo respeto, pareciera que que que como que no aprendemos, o sea y yo no diría nombres, yo no voy a caer en en ese juegos, pero como le indicaba anteriormente, esas personas tienen tanta habilidad en esa delincuencia que se considera una delincuencia especializada. ¿Por qué? Porque no cualquier persona te va a llamar y te va y te va AAA engañar a un punto de entrar en tu mundo de confianza y así extraerte esa información. Por eso es que ese tipo de delincuencias especializadas y no cualquier persona a nivel policial del ministerio público puede abocarse a. A investigar ese tipo de delincuencias. ¿Y es por esa razón de qué? Por supuesto, más intendencias virtuales entran todavía en en nuestra colectividad y eso hace que esto todavía siga en aumento. ¿Por qué? Porque lo ven fácil, es fácil, es dinero fácil, llama llama a una persona ya volviendo a suscitarlos privados y ya les sustrajo su dinero. Esto es increíble, la cantidad de denuncias que ingresan al Poder Judicial Y incluso pasan atrás del centro en el juzgado penal para que el juez determine si la causa se deba ir a juicio o eventualmente dictarse una una resolución diferente a una auto apertura a juicio, como lo hace un sobrecimiento o eventualmente una destimación. Pero eso va en incremento y pareciera que no se detiene, no se detiene, no se detiene y lastimosamente los que están. Se ven perjudicados en ese sentido que son las personas donde ya están adentrándose a su economía y ya entras a la economía de una persona, eso genera un perjuicio grande máximo de que que la todo el costo de la vida es va en aumento. Y eso genera, evidentemente, cuando el juez debe generar un juicio de reproche a nivel del daño creado, la magnitud del daño creado perdón es a través, evidentemente, de la afectación a la economía. De todos y todas las costarricenses donde efectivamente el costo de la vida está alto y esto pues genera perfil, incluso he tenido conocimiento donde yo he tenido la participación de de de conocer casos donde las personas aún estando en el extranjero. Les les les suministra perdón, les se adentran a sus cuentas e incluso les extraen su dinero, no se como, es un aspecto que pareciera que que es una ingeniería de ese tipo de delincuencia. Y es increíble, pero pero si esto va en aumento y va a seguir en aumento, a no ser de que las personas o se abstengan definitivamente. AA recibir mensajes o llamadas de este tipo de de de personas a través obviamente de de de capacitaciones, porque hay que capacitar también a las Personas y es bonito. Y comprar un teléfono inteligente y todo ahora es en el teléfono, usted paga ya, incluso ya no ocupamos las tarjetas. Ya no ocupamos las tarjetas. Ahora el teléfono tiene una aplicación donde usted ingresa al teléfono y usted con un teléfono nada más enseña en el datafono y ya paga. Entonces, claro, facilita mucho en cosas, pero eso es una herramienta fuerte para el delincuente. Y así, evidentemente, pues sustraerle los dineros de los de los y las costarricenses

Orador 1

Claro. ¿Cuál cree usted que es el medio más utilizado para cometer este tipo de delincuencia informática? ¿Entiendese llamada telefónica mensajes o páginas de Internet?

Orador 2

Las llamadas telefónicas porque es el el instrumento más accesible para todos los ciudadanos. Y esto pues toma en cuenta el grupo más vulnerable, como son los adultos mayores. Muy difícilmente un adulto mayor te va. Va a ser tan hábil para acceder a una plataforma como lo es un correo electrónico, tal vez una red social que incluso he tenido participación donde personas venden productos en una red social, Estoy interesado en ese producto. Podemos hacer a través de un número telefónico y ya se hace la vulneración con solo el hecho de auto facilitar por lo menos el número telefónico para acceder al Whatsapp, pero perdón, para acceder al sinpe. Eso pues también es una herramienta fácil para los delincuentes, pero la más utilizada AA consideración del Suscripto es la llamada telefónica. Se hacen, se implementan diferentes porque el delincuente ya sabe, Ah, esa persona no me va a contestar la llamada o qué tal vez con un teléfono, con un mensaje de texto o Un correo. Entonces puede que eventualmente, ya si me torne más seriedad del aspecto, del de lo que le de lo que voy a hacer, que es, es evidentemente adentrar a su economía por plataformas bancarias, pero la vas a utilizar que considero y es la que más utilizas. Es las, las, los, las llamadas telefónicas, claro.

Orador 1

Claro, y supongo yo que también se debe usar en conjunto, hace una llamada, envían un link para poder ingresar a la cuenta del del señor.

Orador 2

Efectivamente, efectivamente, no, eso, eso es una situación. Que se hace de manera incluso conjunta. ¿Por qué razón? Porque ese tipo de delincuencias, las famosas, las conocía como las estafas informáticas, de acuerdo a lo que ha venido a establecer. ¿El jurista y Tratadista Francisco Castillo, en su obra la estafa informática la se le conoce como la estafa triangular, por qué razón? Porque la persona que en este momento está haciendo la llamada no es la misma que está utilizando la cuenta puente y tampoco la que está haciendo la sustracción del dinero. Entonces es una situación tan tan rápida que debe hacerse en cuestión de segundos y es por eso la habilidad que debe tener la persona, porque en el momento que estoy llamando al ofendido, yo estoy en una computadora visualizando lo que estoy haciendo y en el momento donde ya yo le remito. ¿Qué es lo que tiene que hacer? Los pasos le envío un correo electrónico y en el momento que ya lo envíe el correo electrónico, ellos serían una plataforma o una aplicación. Donde ese correo que ellos crean es como un no sé será o un virus OOOO, algo que arrastra la información del ofendido y ya acceden a la cuenta bancaria. Entonces esa situación se hace de manera conjunta con la utilización de otras herramientas como lo son correos electrónicos e incluso a nivel de mensajería de texto. Porque la experiencia que he tenido también me ha dicho. ¿Que yo puedo estar con mi teléfono celular? Y yo creo una plataforma donde yo ingreso mi teléfono celular y cuando llamo a las partes ofendidas para hacer la frustración antijurídica patrimonial, a ellos les aparece un número bancario. ¿Entonces ya hay más confianza aún? Entonces, Ah, me está llamando el Banco Popular ya entró en un en una confianza con la parte ofendida. Entonces en este momento estoy con tantas plataformas abiertas. Para poder acceder, evidentemente, a las cuentas de la parte ofendida. Entonces no solamente esos llamando, sino también estoy en este momento visualizando todo el toda la el sistema bancario en donde yo puedo tener acceso y así poder evidentemente ultrajar a la víctima, entonces es un conjunto. ¿O sea, no se debe, no es el llamarlo decir, bueno, ahora más tarde me meto al correo, no? ¿Eso es llamando enviando un correo y en el momento que ya yo tenga el acceso tengo que hacer hacer los movimientos bancarios, por qué razón? ¿Por qué ahora los bancos están creando sistema de seguridad? Donde le informan al usuario el día tal a la hora tal, en tal lugar se hizo un movimiento bancario que eso es una alerta. Ah no, pero qué está pasando algo y ya cuando llama el Banco AA bloquear la cuenta ya lo ya el el el delincuente me sustrajo el dinero, entonces eso es algo rápido, rápido que tiene que obviamente tener éxito para la delincuencia, por eso es que esa razón es que hay una unidad de voluntades, no solamente el que llama, sino también de las personas que están utilizando las cuentas. ¿Y también puede eventualmente ser qué? Porque

lo que se pretende traer de la delincuencia, no dejar huellas, no dejar huellas, en el sentido de que voy AA sacar este dinero y depositarlo ahí, después yo lo deposito ahí, o sea, estás depositándolo en depósitos, eso va a generar una huella. Entonces llega una cuenta puente y en el momento que llega a cuenta a cuenta ya extraigo el dinero ya físico, o sea en efectivo, para ya después ocultarlo en en otras, ya sea en otras cuentas OOO, no sé. Porque también a ciertas personas de las cual se les pudo vincular. Ese tipo de delincuencias por lo general lo tienen en efectivo, porque sabemos de qué los bancos, a la hora de depositar tanto dinero, les piden ciertas ciertos requisitos para evidentemente evitar lo que se conoce como la la, la legitimación de capitales. Pero por lo general algunos o los tienen en efectivo o directamente lo incursionan en negocios lícitos, para que evidentemente puede blanquear estos activos. ¿Pero más, más o menos, cómo es que ese tipo de personas operan en ese tipo de delincuentes?

Orador 1

¿Claro, entonces en esta delincuencia de estafa informática? Innegablemente tenemos que hablar que existe una coautoría.

Orador 2

Por supuesto que sí, y esa es la dificultad que tiene la Fiscalía en este momento de establecer esa coautoría, por eso es que se deben de requerir. Una serie de herramientas de investigación para establecer ese conjunto voluntades, dice Roxin, a la hora de establecer una coautoría o participación, se den de de establecer una serie de requisitos materiales, como lo es por supuesto. El plan previo, la distribución de funciones y así, evidentemente, tener el dominio funcional del hecho, que eso es lo que establece, obviamente una coautoría o participación. ¿Por qué? Porque la voluntad de las personas es de ese tipo de personas. Es tan importante porque una acción de u otra se acompaña con la otra y para que pueda tener éxito ese tipo de delincuencias, evidentemente el aporte de estas personas es tan importante. ¿Que no podemos aislar? No podemos aislar la acción una de la otra, porque si suprimimos eventualmente la realización del que hace la llamada, no podemos, no puede haber el daño, el resultado parcial total del del del ese tipo de delincuencias se debe contar, por supuesto, con una cuenta a puente, porque si no, entonces no se no se haría el

traslado del dinero. Y por supuesto se debe contar con la persona que ya, porque el delito se materializa, pues de de acuerdo a Don Ricardo Salas en su obra si no me equivoco derecho penal general, el hace una descripción de cuáles son los delitos. De resultado, de mera actividad de mano propia. Entonces quiere hacer referencia que ese tipo de entonces es un delito de resultado. ¿Por qué? Y también lo requiere don Fernando Castillo, porque hasta que el el delincuente tenga el dinero en su disposición, es cuando se hace el resultado del delito. ¿Entonces, por supuesto, si no se ha hecho un retiro del dinero, entonces ya podríamos hablar de un delito tentado, pero como hay éxito en el en la obtención del dinero? Ya podemos hablar de que es un delito que obviamente se consuma. Por eso es que es importante la la Unión de de voluntades en Coautoría, porque hay un dominio funcional del hecho entre todos los que participan. Ninguna acción se puede aislar de la otra. Todas son importantes. Para el aporte realizado para que la delincuencia pueda tener éxito.

Orador 1

Claro, y es que estaríamos hablando en el caso de la persona que hace la llamada, la que está manipulando el sistema, la que retira el dinero, o sea.

Orador 2

Excelente exactamente es ese. Ese esa teoría de participación es lo que hace que ese tipo de encuestas pueda tener éxito. Y, por supuesto, se ocupa la Unión de. ¿Ciertas voluntades de personas igual no sé si lo hará, pero me lo me lo vas a indicar en una pregunta, pero puedo darte un un ejemplo de una de una experiencia que tuve con un caso ya ese caso está resuelto puedo hablar de él? En Puntarenas tuve participación de un asunto que se tramitó como crimen a la criminalidad organizada, donde no solamente se conoció que se se centró a conocer en en ese intervención telefónica lo que eran delitos psicotrópicos la ley de 8204.Homicidios y ya cuando se se ordena, estamos en presencia de de. Un delito de ante una criminalidad organizada y de acuerdo a la ley, al al artículo Primero la Ley de crimen organizado con con sus reformas, donde ya se establezca que hay crimen organizado. Cualquier delito que tenga pena privativa la libertad más de 4 años, entonces ya ingresa, obviamente para que se pueda tramitar como crimen organizado y casualmente esta este tipo de personas se está dedicando a las estafas informáticas. Entonces nos llamó mucho

la atención porque ellos reclutan incluso. Indigentes vaya, saquemos una tarjeta en el Banco. ¿Pero resulta ser de qué? Esas cuentas bancarias del indigente no las va a administrar el indigente, la voy a administrar Yo tengo no solamente el el correo electrónico de ese indigente. Tengo el la clave dinámica, tengo la clave para ingresar a la cuenta bancaria, tengo el simple móvil, tengo el el la banca móvil. O sea, tengo toda la información de esa persona que solamente lo único que hizo fue sacar la cuenta. Y que eso, obviamente, es manipulado por toda la organización criminal. Tengo una persona que tiene habilidad para llamar un poder de convencimiento. Hacia las personas de que efectivamente usted, yo soy un personero de una entidad financiera, una entidad bancaria donde le estoy indicando que ha existido una alerta y por un control de seguridad ocupamos cambiar la la, ya sea la clave, la contraseña y en ese momento que yo estoy haciendo la llamada otra persona. Están en en un Banco X Para poder en el momento en que Yo acceda a esa Información ya está retirado el dinero. Entonces pudimos observar que hay una unidad de acciones, pero que una hay una voluntad y una Unión de tantas personas. Porque si no, ese tipo de delincuencia no tendría exito. Entonces pudimos determinar que efectivamente estamos hablando que era era una organización de más de 30 personas. Donde algunos aportaban las tarjetas bancarias y las que hacían las llamadas que eran dos o 3 personas que tenían esa habilidad y en ese momento histórico, o sea, había en diferentes partes porque eran diferentes estafas que se hacían en ese momento histórico donde retiraban el dinero. Se retiró aquí el retiro, allá retiró aquí el retiro, allá y así después, cuando yo lo fui a cuenta, ya no tiene nada en su cuenta, entonces vemos que no es no depende de la voluntad de una persona, sino que depende de ciertas voluntades para que esto pueda tener éxito.

Orador 1

¿Claro, qué posición le merece? ¿A esa persona? ¿el indigente lo que brinda, es una colaboración o se toma como una participación?

Orador 2

¿Exactamente exactamente, incluso ahí, no?

Orador 1

Que al final de cuentas, don Jordán es la persona más fácil de identificar. Por el tema de la tarjeta.

Orador 2

¿Es correcto? ¿Ahí? Sí, en esa hipótesis sí, porque por qué razón nos dimos cuenta, porque eso fue a través de una intervención telefónica. Eso es lo que te iba a decir, o sea, ese tipo de delincuencias. Y lastimosamente porque los que más se han afectado son los ofendidos. Porque si la Fiscalía es solamente tiene únicamente la cuenta puente. Te lo adelanto, no hay nada que hacer.

Orador 1

Sí.

Orador 2

¿No hay nada que hacer porque incluso el Tribunal de operación de sentencia de San José en una en una resolución, creo que en el año 2022, sostiene que que eso no es suficiente para mantener Participe como coautor a una persona de ese tipo de delincuencias no es suficiente, entonces?

Orador 1

Sí.

Orador 2

Sí, sí, para sí. ¿Para la Fiscalía, que tiene otras herramientas de investigación, pudo estar en el sí, efectivamente, por qué? ¿Porque en ese momento se hablaba mira Johnny, sino es que Jordan me acaba de facilitar la cuenta, anotate ahí Ma, sí, ya tengo la tarjeta Jordan Josue Martínez Cédula tal sí, sí, el Banco Popular, aquí está el PIN, si el me explico, hubo una coordinación porque a través

de la herramienta de investigación de la Internet telefónica se pudo obtener eso, pero si no tenemos eso, no tenemos absolutamente nada entonces. Por supuesto. Si tienes la herramienta de investigación, como la intervencion telefónica tenés no solamente el indigente, tenés al la cuenta puente que efectivamente es el indigente que da una colaboración de acuerdo a la A la participación autoria que sería un posible. Una posible porque sería bueno una complicidad porque no tiene dominio funcional derecho, porque los tienen, por supuesto, lo que es el que hace la llamada y el que utiliza la cuenta puesnte e incluso el reclutador de esas personas. Ahí sí tenés fuerte para poder incriminar a esas personas, pero si no tienes nada que no sea únicamente la identificación del que utilizó la cuenta puente, te digo, no tienes absolutamente nada porque lo utiliza identificado. Sí tienes identificado a la persona que tiene la cuenta, nada más, pero si no tienes nada adicional a eso, lastimosamente es un asunto que no va a poder llegar a podría eventualmente.

Orador 1

Claro.

Orador 2

La parte ofendía podria irse a otra vía, a la A la vía civil Tal vez para poder reclamar eventualmente algún tipo de de daño patrimonial, pero a nivel penal no tienes absolutamente nada.

Orador

No.

Orador 1

Do Jordan desde su experiencia. ¿Usted cree que se logra llevar a juicio o no a las responsables del delito de estafa informática?

Orador 2

En 7 años como juez, el único expediente que pasó el filtro de la audiencia preliminar. Fueron dos causas, una que llevé. En Liberia, y otra que lleve en Puntarenas la la la de Puntarenas fue porque existía una herramienta de investigación telefonica, la intervención. ¿Por qué? Porque en esa investigación teníamos quién hacía las llamadas, porque obviamente eran un acto que se hacía, por decirlo en tiempo real. Escuchábamos cuándo hacía la llamada, escuchábamos Cuándo lo ofendía, contestaba la llamada. ¿Escuchamos en ese momento donde él se le llama Extravos, donde con otro teléfono, mira, sí, sí, sí, ya tengo el dato, te lo ofendí, mira? Mira marcarte salsa. Entonces en ese momento sí teníamos indicios fuertes, no solamente para identificar a la persona que ya sabíamos, individualizada plenamente que hacía las llamadas. ¿Quién eran las personas que en este momento? ¿Hacían las cuenta puentes, el reclutador de las cuentas y la persona que en ese momento estaba haciendo la la el decomiso del dinero, porque la extraccion del dinero por qué? Porque la policía se nutrió todos sus elementos probatorios, que ellos sabían cuáles eran los cajeros que en ese momento estaban. ¿Por qué? Porque las llamadas telefónicas se hacían sí estoy en tal lado. Y entonces, cuando ellos iban a hacer un abordaje policial, les encontraban las tarjetas y los dineros. Que y un asunto que pasó en Liberia parecido entonces la única, las únicas dos causas que yo he tenido participación. Donde pasamos ejemplo para juicio. La preliminar se preliminar para juicio fueron porque se utilizó la herramienta de investigación como la intervencion telefónica después de ahí. Incluso la la Fiscalía de manera muy objetiva sabe que no tiene nada y lo que hace es que pidió una desestimación y pido un sobre, sobre cuándo eventualmente se inauguró la persona que sirvió la cuenta puente, pero él por lo general ellos no se puede establecer. Incluso el diputado tiene el derecho a abstención y no es el imputado que tiene que demostrar su inocencia. La Fiscalía lo que hace es que identifique a la persona, si es que lo identifica, lo indaga, si es que lo indaga, pues por ahí no tiene nada más. ¿Y esas causas? Pues no obtienen únicamente y la identificación de la persona que presta la cuenta. Lo que hace es que objetivamente pide su evento, porque cada vez que no va a pasar el filtro de la audiencia preliminar, entonces las únicas dos causas que he tenido participación son esas dos con herramienta de investigación, como la intervención telefónica, porque sí tenía datos de información de quiénes eran las que hacían las llamadas. ¿Quién retiraba el dinero que no utilizó la cuenta puente que era el reclutador porque se sumaron, además de esa

herramienta, los trabajos de campo donde los los autores policiales que se le encontraban el dinero en efectivo era retirado que se que se que se que se acuerpó con el levantamiento del secreto bancario, porque el levantamiento secreto me va a decir efectivamente qué día, a qué hora, quién sacó el dinero porque se den las cámaras de la persona o donde está saca el dinero? Y a través de otros insumos procesales probatorios, pero como lo es, evidentemente el abordaje policial, donde a fulanito de tal no solamente se les encontró dinero en efectivo sino la las tarjetas número tal porque son el ser, se encontraban más de 15 tarjetas bancarias y así obviamente tenía una una revelación con las cuentas puentes que eran las utilizadas para en el momento que yo retiraba el dinero, trasladarla a la cuenta de los de de las personas que eran colaboradoras para hacerla para hacer como el pasaje o el puente de los dineros y así posiblemente se retirados.

Orador 1

Claro. ¿Se declara siempre delincuencia organizada en este tipo de delitos o no? ¿Justamente porque la herramienta parece más efectiva es la intervención telefónica, por lo menos para localizar a alguien más, verdad?

Orador 2

Exactamente, pero si hacemos un análisis de la ley 7425, que es la ley de registros secuestro en su artículo 9. No establece como requisito sine qua non por un aspecto de legalidad que ese tipo de de delincuencias no se aplique. Para solicitar de. Manera directa, obviamente sí. ¿Quiénes son los participes para poder investigar? La ley no permite por lo menos prima fase, como como la lista taxativa de delitos que permite esa herramienta. A no ser. Que ya se ha decretado y ordenado la delincuencia organizada y se pueda agregar esa delincuencia en la herramienta de investigación, porque lo declarado crimen ahí entra incluso amenazas agravadas, lo que sea por decirlo de esta manera, o sea cualquier delito que tenga pena de prisión, por ejemplo, un delito de más de 4 años entra en la herramienta de investigación siempre y cuando sea declarado crimen.

Orador 1

Claro. ¿Cómo consideras el trabajo del Ministerio público y de la Policía Judicial para la obtención de prueba para el delito de estafa informática?

Orador 2

¿Yo siento que la Fiscalía y el Ministerio público en ese sentido, saben? Que como no va a pasar el filtro de la audiencia preliminar, si lo único que cuento nada más, es la identificación del del del. Que del que brinda la cuenta. Para la opción de dinero, ellos, o sea, no hacen una labor más allá porque saben de que no va a obtener nada más. Porque sé que es lo que nos va a decir la el el levantamiento del secreto bancario. Sí que ese dinero pasó a esa persona y esa persona retiró dinero y ya no sabemos nada más. Entonces hay jueces. He visto resoluciones de jueces donde incluso. Solamente se tiene la denuncia de la parte ofendía y la parte ofendía a cuerpa de su denuncia lo que son los movimientos bancarios. Y he visto resoluciones de jueces donde si el fiscal refiere la estimación de la causa porque solamente tiene eso, lo lo ordena. Hay jueces que le piden. Un poquito más a la Fiscalía ya no importa, no, no, no. O sea hacer por lo menos el levantamiento secreto bancario a investigar un poco más, aunque tenemos el levantamiento secreto bancario y ya no tenemos nada más. Entonces creo que la Fiscalía incluso es consciente de que como no hay otra otra herramienta más que investigar, lo que hacen es que dejan de investigar y piden que la causa se archive porque no es que yo se lo ataque alguna responsabilidad, porque sean negligentes o porque eventualmente no quieren investigar, es quien no tienen más que hacer y no te pueden pedir una intervención telefónica porque no da para que la causa sea eventualmente por esa herramienta de investigación, porque la misma ley lo prohíbe solamente este tipo a no ser que se reforme la ley y que eventualmente puede aplicarse este tipo de delincuencias a nivel cibernético oh a nivel de informático.

Pero no es porque la Fiscalía no quiera investigar, sino es que no tiene más que hacer y lo único que nos va. ¿Incluso he visto casos donde piden el levantamiento secreto bancario y lo que el Banco dice, cómo ha sacado, como esa extracción o sustracción? Pero se dio hace más de. Mes, porque a veces se acuerpan lo que son las cámaras de de de los de los de los cajeros. Donde dice el Banco no, no se pudo aportar a las cámaras porque ya eso pasó hace. 3 meses y el y el formato solamente guarda por dos o un mes

Orador 1

Ajá.

Orador 2

Entonces ya tener ya ya ya por lo menos no puedes hacer una comparación de de personas físicas con fotografía, ya no tienes eso, lo unico que tienes es el movimiento bancario y después de no tienes absolutamente nada más. Entonces, por más de que la Fiscalía quiere investigar, no va a pasar de filtro. No es que sea una responsabilidad de la Fiscalía, sino que ahora la política de persecución penal en violaciones a delincuencia no da para que las herramientas de investigación que cuenta la Fiscalía o el OIJ pueda eventualmente ser utilizado para poder seguir o continuar con la investigación, sino que esto es vago, sea la los recursos son vagos y al ser vagos entonces no hay, no hay más allá el del del recurso humano. Que pueda ser utilizado para que se pueda investigar, por lo cual en ese sentido no es que justifique a la Fiscalía que no investigue esa delincuencia, sino que en este momento no cuentan con una herramienta más de investigación para poder establecer una posible participación efectiva de ese tipo de delincuentes.

Orador 1

Claro. Don Jordan y en el caso de la pieza acusatoria, cuando logra presentarse. ¿Cómo se puede determinar o más bien si ha tenido la experiencia? ¿Cómo va en tiempo, modo y lugar la pieza acusatoria?

Orador 2

OK, eso es muy importante porque hay que recordar de que la la acusación fiscal, de acuerdo al 303, debe de tener debidamente establecido un aspecto que usted acaba de indicar importantísimo. Circunstanciación en tiempo, modo y lugar. ¿Por qué? Porque es de ahí donde se hace una correcta imputación de hechos. ¿Para qué? Para que no vulnere el derecho de defensa. Es muy importante

que el diputado debe saber que ser esté acusando, por qué se les está acusando, cuál es el motivo de la acusación y cuál es la prueba que sustenta la acusación. Entonces, si la parte diputada conoce esos aspectos y puede ir, puede eventualmente la audiencia preliminar, ya sea pedir el sobre, porque evidentemente yo puedo refutar la prueba, puedo pedir sobre el decreto o incluso en el en la etapa al contradictorio. ¿Entonces, cuál es la Circunstanciación en tiempo, modo y lugar que la Fiscalía debe hacer primero? El plan previo. Desde la teoría del delito conocemos el iter ciminis o el análisis del intercriminis, la ideación del plan, lo que yo en mi psiquis estoy creando, estoy imaginando, estoy planeando para poder ingresar a las cuentas de la parte ofendida, extraer su información y así posteriormente. Sí, evidentemente, poder hacer la extracción de sus de su dinero de manera antijurídica, ese es el plan previo. La distribución de funciones, porque ya nos dimos cuenta que solo la persona que llama no puede, evidentemente hacerlo solito, entonces cuando hablamos de plan previo y la identificación tenemos que establecer. ¿Qué fueron sutano, mengano y parenceo? Tenemos identificación de 3 personas. El plan previo el plan previo es que yo idee un plan para acceder a los datos y extraer el dinero, distribución de funciones. ¿Quién llamó? ¿Dónde fuera a dar el dinero? ¿Quién retiró el dinero? Eso es. Importante porque esos aspectos ya me van a decir lo que es la autoría y la coautoría. El autor tiene el dominio de la acción y el coautor que realiza la acto en en en coordinación con el autor tengo el dominio funcional del hecho. Entonces esos aspectos me va a dar a mí a decir que la acusación está precisa. Circunstancia. Y evidentemente está bien fundamentada para poder yo decirle al juez penal, señor juez, esas tres personas idearon un plan previo para acceder a la cuenta del ofendido, y una vez teniendo y manejando y en su posesión los datos sensibles del ofendido, ingresaron a su cuenta bancaria, hicieron una sustracción del mismo, la cual Jordan Martínez que se abocaba a realizar la llamada al ofendido. Don Rodríguez Rodrigo Castro Méndez, en la cual en ese momento histórico donde Jordan ya tomó en posesión, dominó la voluntad del ofendido, lo hizo entrar en confianza, en la cual efectivamente eso con su investidura de funcionario del Banco, lo convenció de que efectivamente usted ha sido víctima de un posible fraude. Entonces ocupo sus datos para poder hacer el cambio de cuenta, cuando en ese mismo momento la persona identificada como Johnny Rojas está utilizando su cuenta puente para que posteriormente don Asedio Vargas realice la sustracción del dinero entonces. ¿Esa acusación? Viene a establecer una circunstancia de un tipo oruga porque fue el día 12 de enero del año 2023, al ser aproximadamente las 4:00 H cuando no sabemos. en donde Jordanhizo es una llamada, pero sí sabemos dónde se retiró el dinero, entonces sí hay un aspecto, en cuánto tiempo, modo y lugar,

hay resultado del delito, hay una Circunstanciación en tiempo, modo y lugar, hay una realización en cuanto una dinámica y esto da fuerte para que una en una acusación la misma pueda sostenerse en en una audiencia preliminar y pasar el filtro, Por supuesto, a un posible juicio oral y público con el dictado de un auto apertura a juicio. Obviamente lo que sería aportar son los elementos de prueba, como lo es por ejemplo si se utilizó una herramienta de investigación como lo es la intervención telefónica, que pareciera que es la única forma la cual en este momento enfrentar a una realidad procesal, lo que lo que podía contar a la Fiscalía para poder identificar a esas personas. Trabajos policiales de de de OIJ, como son vigilancias, trabajos de campo. El levantamiento secreto bancario, la denuncia del ofendido, sus movimientos bancarios, de sustracción y, entre otros, análisis que puedan hacer aportados por la delincuencia organizada. perdon por la ciberdelincuencia por parte del OIJ sobre este tipo de delitos que son delitos informáticos, sería la única forma en cómo yo podría valorar que efectivamente hay creces probatorios para poder pasar ese filtro. Si la Fiscalía me dice es que únicamente no sé quién llamó, no sé quién retiró el dinero, pero sí sé que Jhonny Rojas utilizó la cuenta puente, créame que eso no va a pasar el filtro.

Orador 1

Por supuesto.

Orador 2

¿Sabemos sabemos cuando llamaron al ofendido? ¿Sabemos cuánto fue el dinero que se le sustrajo? ¿Sabemos eventualmente cuál fue el medio idóneo que fue una llamada telefónica? Sabemos que eventualmente se utilizó a través de un correo electrónico que no sabemos cuál es la dirección IP, pero sí el el correo electrónico que lo ofendió ingresó y se le sustrajo, es lo único que tenemos. Pero si eventualmente no sabemos quién llamo quién tiene el dinero, entonces no hay, no hay, pues no se puede establecer el plan previo y la distribución de funciones. Y eso créame que en una preliminar es tan débil que cualquier juez, incluso ese servidor, podrías dictar un sobreseimiento definitivo porque no tienes nada. No tenías nada para llevar ese juicio a ese proceso a juicio, y muy probablemente se le pueda dictar un sobreseimiento definitivo por duda, porque no se ha hecho esa conexión. El plan previo, distribución de funciones y la materialización del hecho delictivo.

Orador 1

Claro. ¿Entonces sería? Bajo lo que usted me está diciendo, son muchos los casos que existen un sobreseimiento.

Orador 2

Sí, sí, bueno, como te dije anteriormente, desde el año 2018 más o menos que he tenido más aporte en. En ese tipo de delincuencias, créame que. Si le digo que he dictado más de 500 te miento pueden ser entre unas 800 a 1000 sentencias de sobreseimiento definitivo bajo esa tesis y que la misma, pues ha tenido su su sostenibilidad en el en la etapa recursiva, o sea, en apelación porque lastimosamente lo que tenemos es vago para investigar. ¿Entonces quién es el más afectado la víctima? Caso que ingresa por estafa informática La Fiscalía sabe que no va a tener un proyecto a no ser de que se incorporen más elementos probatorios, pero si solamente tenemos denuncia y cuenta puente. Eso va con un dictado de una desestimación muy probablemente.

Orador 1

No pasa.

Orador 2

No pasa, no pasa el filtro.

Orador 1

¿Además de lo que hemos hablado, cuál es? ¿Cree usted que son los principales obstáculos que dificultan esa identificación del ciber delincuente?

Orador 2

El principal, el primer obstáculo que tenemos es la forma. Cómo tenemos para investigar el primero no obtenemos por lo menos si es a través de una. Llamada telefónica, en la cual pues a no ser de que lo ofendido pueda grabar la la llamada en ese momento. Saber quién es la persona que evidentemente los llamó porque sabemos de que ninguna, ninguna llamada en ese sentido se graba a no ser de que pueda ser peticionada por una por parte de de de la intervención telefónica. ¿O sea, sabemos de que si usted si usted es un mismo momento me está llamando? A no ser de que yo ella le diga a mi pareja, me está llamando esa persona, no sé quién es, grabémosle la voz, a través de un reconocimiento de voz tal vez podría eventualmente establecerse bajo una investigación, darle continuidad a ver quién es la persona que llama, pero en este momento, lastimosamente, cuál son los obstáculos? Identificar primero quién es el que llamo. Es el primer obstáculo. No sabemos quién es el que llama, no sabemos donde está ubicado porque el único registro a no ser de que se pueda activar radio bases. Y es que eso es otro aspecto esas personas son tan inteligentes que no utilizan radio bases, o sea, no conectan el Internet. ¿Para qué? ¿Para no bajar huellas? ¿Porque yo puedo pedirle OIJ que haga un registro de radio bases, sí, pero la radio base me va a decir dónde está ubicado el el teléfono y que qué hago con eso? O sea, lo único, lo lo lo único que me ha tenido una radio base es que sí te borra el registro de bases, en corredores propiamente cerca de río nuevo, en río nuevo, en Rio Nuevo es donde viene mi pareja, para que me puedan entener en río nuevo hay un montón de casas. ¿Cuál casa? O sea, eso no es suficiente. Entonces el primer obstáculo es identificar a la persona que hace la llamada, porque si identificas a la persona que hace la llamada, ya puedes trazar un lazo o trazar una conexión ¿Tal vez con la persona que brinda la cuenta puente, tal vez no al que retira el dinero? Pero sí hacer una conexión con la persona que hace del primer la cuenta puente para hacer un trazo. Y EH, perdón, indiciariamente decirme que efectivamente hay una coincidencia de que la persona que llamó. Tiene un fuerte, una fuerte conexión con la la persona que hace la cuenta puente, entonces Indiciariamente pues amarrarlo, entonces al el obstáculo, ahorita es primero que no tenemos una herramienta de investigación fuerte, Para poder identificar a la persona que evidentemente hizo la llamada, no sabemos, no sabemos a través de un reconocimiento de voz acuérpalo con otros insumos procesales, un momento nada más para abrir la puerta.

Orador

Claro

Orador 2

Entonces ese obstáculo, como yo lo puedo visualizar, es primero identificar a la persona que hace la llamada, porque no tenemos en este momento alguna herramienta que pueda identificarlo, a no ser de quien ofendido sepa no, no hay algo raro, eso me parece que una escafa. Entonces él fue a eventualmente grabar.

A la la persona que lo está llamando en ese momento y así poder lentamente establecer una una conexión en cuanto a reconocimiento de voz, porque si pensáramos en una intervención telefónica ahí sí podríamos tener es porque ya. Policialmente se sabe quién es la persona que presuntivamente y manera sospechosa bajo una información confidencial, sea la persona que ha estado llamando y a raíz de eso sí hacer el trazo con la herramienta de investigación, pero ahorita el obstáculo es identificar a las personas que llama porque no tenemos nada, o sea, no se puede ahorita en este momento identificar a una persona con una sola denuncia para por lo menos seguir un trazo, un trazo de investigación, y eso es lo que obviamente en ese momento es lo que mantiene una cantidad de expedientes con sobrecimiento definitivo, a razón de lo que ya hemos estado hablando, pero el obstáculo primero es eso, y. Individualizar a la persona que hace la llamada porque después de ella no tenes absolutamente nada más, entonces y pensar eventualmente en herramientas de investigación. La única que nos podría venir a dar es insumo probatorio es la la la intervención telefónica nada más es la única, pero después de eso no hay nada que me pueda ir a decir quién llamó y quién era la persona que evidentemente está haciendo la llamada.

Orador 1

¿Claro, a nivel tecnológico, ahora que estamos conversando, qué tecnología es su herramienta? Considera usted que podría ser también útiles para mejorar la identificación del.

Orador 2

OK en primera instancia, la herramienta de la intervención telefónica, porque la herramienta de la intervención telefónica tiene puede captar obviamente grabar la voz de la persona y, a través de un reconocimiento de voz, identificarlo. ¿Creando una base de datos, verdad? En la cual todas las personas, cuando se hace una consulta a nivel policial, más si se ocupa identificar a esas personas. Pero seguramente tengo la voz, entonces ese reconocimiento de voz se puede dar por lo menos ciertas similitudes. OK, me salió, que tiene la voz parecida y eso me permite investigar. Qué investigar o qué está bien haciendo conexión de radio bases, haciendo un trabajo de investigación. ¿O sea, qué otros elementos más informaciones confidenciales, si eventualmente hacerle algún tipo de de perfil a nivel criminológico, o sea, si se le ha envuelto, visto envuelto en ese tipo de delincuencias, qué habilidades pueda tener la persona también a nivel de conocimientos bancarios? Por qué, La experiencia que he tenido a nivel policial también se tuvo información de que, como lo indique anteriormente, esas personas no llaman a alguien así al azar. ¿Sabes a quién llamar entonces? Se ha indicado también que en apariencia hay funcionarios del Banco donde ellos tienen conocimiento. Qué personas tienen capa, tienen capital y les aportan información. O sea, Mirad, Jordan, según Vicente, que está doña. Se acaba de jubilar ¿Y no, y más bien nos llaman a cada rato para que le estemos haciendo movimientos bancarios, porque sabía que efectivamente esa doña es fácil de manipular, tome se llama tal tal, tal por eso es que uno a veces queda asombrado por cómo este man está llamando, sabe dónde trabajo, sabe todo de mí, entonces entonces definitivamente esa persona es una funcionaria del Banco, por qué? Porque me está llamando con esa investidura y tiene mi información y por esa zona de que es fácil, Para ellos es fácil utilizar este medio YYY así evidentemente generar el el. El el el generar el el daño patrimonial y antijurídico que es la sustraccion el dinero. Entonces. Ese tipo de modalidades de la herramienta de investigación, como la intervención telefónica, puede reconocer la voz de las personas. Eso generaría qué generaría conectes trazos como lo llama la policía, o sea, la policía hace trazos para poder establecer, evidentemente ese esa, esa unidad de voluntades y así en una en un en una posible acusación, establecer la distribución de funciones. En Estados Unidos yo sé que se utilizan mucho el el reconocimiento de voz y me pareció muy curioso porque hace Yo no había ido, no había visitado ese país y hace como 2 años en la paz yo me quedé asustado Ellos no te piden el pasaporte, ellos no se dejan ni le sellen el pasaporte a uno, ellos únicamente ellos lo ven, lo y pero antes de pedir el pasaporte a uno Hay una, hay un sistema que ellos tienen donde usted se pone como una Cámara

ya la Cámara ya lo vio usted lo exactamente ya lo reconoció facialmente e incluso usted hablando ya ellos saben quién es usted.

Orador 1

Biométrico.

Orador 2

Entonces vemos que esa ese tipo de herramientas a nivel informático o de delincuencia organizada, como ese tipo de modalidades, podría ser un arma para poder identificar quién es la persona que evidentemente está haciendo la llamada y como esa persona sabemos, esta haciendo la llamada con una conexión de radio base y la ubicación porque ellos eso es un perfecto. Cuando usted hace las llamadas ellos pueden identificarlo. A usted donde usted hizo la llamada no diferente de aquí que lo que se hace es que hay un registro. En Estados Unidos, independientemente si usted bajo una intervención telefónica o no, usted hizo una llamada. ¿Ese registro le dice a la persona o a los policías o los oficiales, dónde se hizo la llamada? ¿Aquí no, yo lo puedo llamar a usted y el único registro que hace es que sí, efectivamente yo lo llamo a usted, pero dónde? No sabemos por qué, porque el único rastro que puede dejar dónde se hizo la llamada es a través de radio bajas y es a través de la aplicación la implementación de datos móviles que es el Internet y entonces esos aspectos también podrían ser ubicar OK pesar de que la línea. ¿O sea, que esa gente compra en líneas, verdad? ¿No son de ellos entonces?

Orador 1

Sí.

Orador 2

Si eventualmente el reconocimiento de voz dijo que la voz se parecerá de Jordan. Y los puntos desde que la llamada fue fue fuera en río nuevo, pero yo ahora no vi en río nuevo, Sí, pero vive la pareja y Jordán está ahí. Entonces ya tienes eso, tenés el reconocimiento de voz, tenés que efectivamente Jordan está aquí y que Jordan. Y como una prueba de tenencia, que es prueba de tenencia, donde la policía llama. ¿Buenas, con quién hablo? Habla con Jhonny Rojas y corta. Debe decir que va a tener. Ya ya hice positivo. Fui seguro entonces con cartel esos esos, esos, esos, esos elementos. ¿Tenés el reconocimiento de voz, tenes la ubicación donde se hace una llamada y la prueba de tenencia, que efectivamente vos sos el que estás haciendo la llamada porque la prueba de tenencia de la policía está en un punto estratégico, donde lo ven que usted saca hace el teléfono, entonces usted lo está usando? Entonces es usted que hizo la la la, por supuesto, la llamada telefónica, entonces con base a eso puede ser eventualmente una herramienta de investigación. AA tomar en cuenta para analizar en ese tipo de delincuencias, pero obviamente se se ocupa el recurso y el recurso no es nada barato.

Orador 1

Por supuesto, dentro de lo que me ha dicho ya dos veces, es la parte de. ¿De quién provee los datos? ¿Porque efectivamente, como usted dice, cómo sabe el que me está llamando primero que yo soy cliente de ese Banco? ¿Que yo tengo dinero en ese Banco porque si no tengo que filtrar para saber que la posible estafa vaya a ser efectiva, si no hay dinero, de qué le sirve la llamada?¿Qué qué interesante eso, quién da? Del cliente o de la posible víctima.

Orador 2

Sí, ahorita bueno y te voy a hacer muy transparente, sé que esos son para fines meramente didácticos, porque tampoco se puede comprometer una investigación penal que esté en curso, pero fíjate que a pesar de que las las dos causas que yo te he dicho, en la cual ya tiene sentencia. ¿Nunca se pudo establecer policialmente quién es la persona? No, pero se sabe que en apariencia es una persona del Banco, no sabemos quién. y podemos especular, Daisy, puede que sea tal vez alguna muchacha enamorada de algún criminal ahí que le pase datos o que yo eventualmente le diga al mae del Banco, mae, mira, pásame datos y yo te paso una mensualidad.

Orador 2

O eventualmente que sea un primo de alguien o familiar de alguien, pero que el dato sale del Banco sale del Banco, porque como te digo, o sea, yo puedo tener habilidad para manipular datos, Johnny, pero cómo yo voy a saber porque. Yo no sé por más de que yo me meta a usted en el registro, yo no sé de qué banco es usted.

Orador 1

Correcto, no hay forma.

Orador 2

Yo no sé qué van con ustedes, no sé qué cuánto dinero tiene usted, no sé cuál. ¿Es su correo electrónico que usted está usted está aplicando en el Banco? ¿Pues yo tengo 3 problemas electrónicos, pero cuál es el específico que está en el Banco? Todo eso es información que sale del Banco, Lastimosamente, pero OK, no se han podido establecer.

No se ha podido establecer quién quién puede proveer esa información, pero sí sabemos de qué esa información sale del Banco.

Orador 1

Por supuesto, más bien son muchos los autores se quedan fuera el que realiza la llamada, o sea, todo el que hace la ingeniería social, el que brinda los datos, el que manipula el sistema, el que saca el dinero o recluta para sacar dinero.

Orador 2

Exactamente no son varios, es todo una criminalidad organizada que incluso yo en Liberia, yo en Liberia ordené y Decreté. Una criminalidad organizada bajo esa modalidad porque incluso me acuerdo muy bien. ¿Dónde unos unos chavalos se habían metido a robar a la casa de una señora? vea la ingeniedad de esas personas, donde. Se sabía que esa persona tenía cuenta dinero en su cuenta y resulta ser de que la llamaron toda la modalidad que le he dicho, la llaman su cuenta ha sufrido una posible afectación. Hay que cambiar la clave y ella aporta datos sensibles. Se les sustrajo el dinero y posteriormente a todo eso, ella llamó al OIJ e interpuso la denuncia. Y resulta ser de que la las personas sabían que había interpuesto una denuncia y habían ido unos oficiales a la casa de ella y se identificaron como oficiales de Policía Judicial de la ciberdelincuencia, pasen muchachos, claro que sí. Que no eran los mismos criminales que le habían llamado y le robaron todo lo que había en la casa, joyas se le robaron como dos carros, o sea, vean todos los datos que esta gente maneja. Manejan para evidentemente sí ultrajar cualquier a cualquier persona. Entonces vemos que hay una unidad de voluntades de tantas personas que por supuesto hay una criminalidad organizada. La criminalidad organizada por el artículo primero artículo de la ley a crimen Organizado, establece que debe existir una intervención de 2 o más personas, por supuesto tener. De 2. Hay una unidad de acciones que esas personas se avocan. Ah, efectivamente vi a tener una especialidad en esta delincuencia y otro al tanto que yo valoré, si no me equivoco también. En en en en esa jurisdicción que yo estaba. Es que se pidió radio bases y las radio bases sí estblecia que las personas que estaba llamando sí se mantenía en esa cercanía y que eran de la zona de de Guanacaste no me acuerdo muy bien. Y que además, la persona siempre se identificaba como el mismo seónimo. Que obviamente no va a decir que soy yo, mira, así habla Juan José Rodríguez, del Banco Nacional, que era el mismo, era la misma persona que se identificaba y entonces ellos empezaron a hacer un como un trazo ¿Por qué? Porque ellos sí fueron inteligentes, ellos vieron primero la criminalidad organizada. Y decretar la criminalidad organizada que sí podían pedir después.

Orador 1

Intervención telefónica

Orador 2

¿La intervención telefónica porque ya ya hay, ya hay crimen y ahí si Pegaron al mae

Orador 1

Claro, sí, hacen un rastreo de llamadas previas y pueden.

Orador 2

Pero es. Exactamente, YY esas personas ya habían estafado. Como a 8 ó 9 personas más, entonces ya habían 9 denuncias. ¿La misma dinámica? Era la misma cuenta puente y entonces y e ingresó la información confidencial, que era que era tal persona. Entonces, todo ese rastro lo que pudo establecer es que, efectivamente, Martínez era la persona muy probablemente que. ¿Que hacía las llamadas? Pero hay que corroborarlo y la única forma de corroborarlo era a través de la intervención telefónica y no las dan. Entonces, ahí sí. Por lo menos el artículo 9 no dice que ese tipo de delincuencia se pueda, pero como se decreto crimen, entonces sí se pudo aplicar la la estafa informática y sí se aplicaba y se pudieron acuerpar para otros datos adicionales como lo era. De los trabajadores policiales, los decomisos de los dineros, los decomisos de las mismas tarjetas, entonces, en fin, ahí se fueron como 30 personas ahí detenidas.

Orador 1

¿Claro, don Jordán en esto es una delincuencia muy doméstica o es muy internacional?

Orador 2

¿Es internacional? Bueno, a por lo menos aquí aquí en Costa Rica, por lo menos lo que yo sí he experimentado es una delincuencia por lo menos común. Aquí es territorial, pero ajá, exactamente, pero exactamente, pero sí he tenido por lo menos.

Orador 1

Doméstica de Costa Rica, el delincuente es de Costa Rica.

Orador 2

Conocimiento, no participación, conocimiento que hay incluso a nivel internacional, personas que tienen cuentas en el extranjero. Verdad, donde igual son trabajadas por lo mismo datos que salen de aquí de Costa Rica. ¿Pero eso es lo que yo también he escuchado, no me consta, no he tenido algún tipo de participación, pero pero sí sí como son aspectos de de índole informático Yo puedo abrirme una cuenta ahorita un Banco X yY bien bien me pueden, me pueden, me pueden estafar entonces, Bien, pues voy a pensar así, pero a nivel de experiencia lo único que he podido tramitar es es obviamente aquí en Costa Rica, pero. Yo siento que si es complicado tramitar un asunto aquí en Costa Rica, imagina de Corte Internacional, claro, entonces yo siento que ahí sí debe haber un aporte. Más atrás de las autoridades para poder establecer ya. Ir porque esto esto esto parece no acabar y es muy y es y es y es. ¿Es lastimoso porque y cuántas denuncias no ingresan todos los días al OIJ por estafas informáticas? Yo he visto denuncias de más de 5, 10, 20 millones de colones y es que claro, yo tengo mi cuenta para ser SINPES por 500000 y. ¿Me puedo meter a la banca móvil y puedo modificar eso? ¿Los 100, los 10 000 000 de pesos, es un ejemplo que yo pueda tener en mi cuenta, los puedo trasladar a su cuenta? Y bien pasan.

Orador 1

Cierto.

Orador 2

¿Bien pasa?

Orador 1

¿Don Jordán, qué tipo de investigación debería implementarse en estos delitos informáticos?

Orador 2

La primero que todo pensaría Yo, esto pensando en el bien común, no en el bien individual, porque sabemos de que uno de los fines del del Derecho público es el bien común, y el bien común es la colectividad y pensando en la colectividad. Es que habría que modificarse la ley de estafas, perdón, la ley de registro y secuestro, que sé que si hacemos un análisis del artículo 217 bis, por lo menos en su en su segunda, en su segunda. ¿Segundo párrafo que hace un aumento en cuanto a la oximetría penal, que ya estamos hablando, no? Un delito de que va de 3 a 6 años, sino que sería de 5 a 10 años. Cuando ya son vulnerados los sistemas bancarios, entonces eso permitiria por un aspecto de proporcionalidad. Pensar eventualmente en que se puede aplicar o ampliar la gama de delitos para investigar en cuanto a las intervenciones telefónicas, lo que es la estafa informática o elementos informáticos. ¿Por qué? Porque esta especialidad, particularmente, incide en aspectos, obviamente. informáticos que como lo indiqué anteriormente, cuál era la que más se explica? El aspecto telefónico, la la estafa que más regularmente se aplica. Yo llamo, entonces pienso yo que por la dinámica en la cual se desenvuelve esta delincuencia y también por la forma en cómo está estructurado el tipo penal, que es un tipo penal que va de 5 o 10 años, por un tema de proporcionalidad y pensando en el bien de la colectiva, porque esto parece que va en más aumento, esa herramienta de investigación podría incluso. No solamente reducir primero. Investigar y dar con las personas que tienen participación en esta, sino que también podría ser un aspecto de reducir. ¿Evidentemente ese tipo de delincuencia por qué? Porque recordemos que los tipos penales. O el Derecho penal se creó no solamente para. ¿Que puede hacer una alerta para las personas? O sea, tengo un supuesto. De hecho, si yo doy muerto a una persona, tengo una consecuencia legal que sería de tanto a tanto. Entonces ya es una alerta para mí. Entonces, si yo sé que la estafa informática puede ser investigada por la intervención telefónica, creo que cualquier persona no. ¿Realizaría ninguna llamada? ¿Por qué? Porque mi voz se queda registrada ya mi voz a través de reconocimiento de voz. Ya sabemos quién va a ser. Entonces creo que ese delito por un aspecto de política criminal se reduciría y creo que me podría atrever a decir que nadie generaría. ¿Nuevamente voy a llamar a Jhonny para estafarlo, saben que de dónde viene la llamada, saben?

¿Quién fue el que llamó, mi voz está ahí a nivel judicial, entonces creo que la herramienta de investigación, como lo es la la intervención telefónica, el reconocimiento de voz e incluso implementar lo que se conoce como el famoso rastreo por GPS. ¿Dónde fue que salió la llamada? ¿Entonces? Creo que podría ser efectivamente una luz fuerte para la investigación de este tipo de delincuencias y que incluso a nivel internacional Estados Unidos colabora mucho con Costa Rica, Vea que véase que el centro de intervenciones fue dado por los por por el Gobierno americano para para perseguir obviamente delincuencias bajo la ley en su artículo 9 y establecer obviamente bajo llamadas telefónicas, quiénes son las personas que podrían haber tenido una cierta participación en derechos, obviamente por considerarse grave, pero esta podría ser por lo menos una forma de respuesta a la colectividad. En la investigación de esta delincuencia.

Orador 1

¿Debería crearse un cuerpo policial especializado en este tipo de delitos?

Orador 2

Sí, claro, por supuesto, como le indican anteriormente, Francisco Castillo dice que los delincuentes tienen habilidad del manejo de ese tipo de de sistemas para la consumación de esta delincuencia y si estoy, estoy tratando con una persona que tiene un alto perfil de conocimiento del sistema bancarios. Por supuesto que la persona que investiga a nivel de dirección funcional, Ministerio Público y el cuerpo policial que ejecuta actos de investigación, deben de tener conocimientos informáticos. ¿Por qué? Porque hay al yo saber cómo se manipula un sistema informático. Yo puedo crear también aspectos de cómo puede perseguir a esa persona, porque mentiras, y te lo digo con todo respeto en el Ministerio Público la famosa frase es uno, solo si yo puedo eventualmente estar en delitos ambientales, no sé nada de informática. No voy a cubrir una suplencia ahí es que ocupamos llenar un campo como una persona que no tiene conocimiento de informáticas. ¿Por qué? ¿Porque lo único que voy a decir, Ay, pero qué hago aquí? ¿Cómo investigo esto? Mirada oficial o. Han de acompañarlos a los simples, mandemos a preguntar eventualmente Day, un levantamiento cierto bancario, a ver qué nos va a dar al no tener una especialidad, al no tener un conocimiento específico en el tipo de delincuencias. ¿Por qué? Porque la el único, la única, el único

equipo que tiene un OIJ hasta ahorita a nivel informático es el cibercrimen, el cibercrimen son peritos. El crimen lo único que te voy a decir es que se sabe. Información, pero. A nivel de llamadas, a nivel de investigación, a nivel de rastreos, todo eso lo que hemos estado hablando, personas especializar en ese tipo de delincuencias son los que deben de investigar y por supuesto crearse esa ese cuerpo policial, crearse ese ámbito en la Fiscalía que porque si hablamos de derechos informáticos hablamos de todos los delitos informáticos, no especialmente en la estafa informática, que es lo que me ha correspondido, porque y lastimosamente en la Fiscalías todos los fiscales que que presentan solicitudes son descargadas, que no tienen conocimiento en qué es, qué es lo qué podemos conceptualizar y, por lo menos, en en un concepto para la redundancia, que son aspectos informáticos. ¿Qué, qué, qué es un sistema bancario? ¿Qué es el sinpe móvil? O sea, no. Un fiscal le llega una causa ahh estafa informática denuncias, esto va para solicitud de desestimación. Sabemos de que la herramienta no va para más, pero si eventualmente. Se cuenta con una intervención telefónica a través de eventualmente crimen organizado. ¿Que podemos hacerlo así? Sí puedo, eventualmente a través de de investigación que puedan acuerparse o ser solidificados aspectos informáticos. Creo que sería una herramienta muy útil para para los que se encargan de perseguir este tipo de delincuencias, por lo cual. Claro que sí, claro que debe existir una sección especializada en ese tipo de delincuencias, porque si usted me pregunta a mí, yo puedo tener conocimiento en derecho, pero usted me pregunta a mí, yo sé manipular un sistema o cómo digo? Obviamente estaría mintiéndole que no sé, no sé cómo hacerlo, porque para eso se se se requieren personas especializadas para tal efecto.

Orador 1

Correcto, Don Jordán ¿Qué recomendaciones generales tiene para mejorar la identificación del ciberdelincuente dentro de lo que hemos conversado?

Orador 2

OK. Como primera mano se deben mejorar la forma de investigación. Por supuesto, la forma como se investiga ahorita es una, es una forma de investigación vaga, esto genera impunidad, es por supuesto y también genera a di que genera en la imagen del Poder Judicial. ¿Decepción porque

cuántas personas van a estrados judiciales? ¿Para mantener el gran derecho que se le ha sido menoscabado, pero resulta ser de que se grandes decepciones, porque qué lo quiere decir la Fiscalía? No es que no se puede ni identificar a la persona que llamó entonces el caso está archivado. Y esa decepción genera que las personas ofendidas, sí, sí, me robaron la plata y me van a seguir robando y no pasa nada. La forma como se investiga también un aspecto de mejora en ese tipo de. De este tipo de delincuencias también podría pensarse. En la forma como se crean las sesiones de investigación, como le indiqué anteriormente la sección de OIJ especializada, la sección de Ministerio Público especializada también en ese en ese efecto también otro aspecto de importancia que se que se puede eventualmente valorar en ese tipo de de delincuencias. La hora. De investigar es que el Estado pida colaboración internacional. Los estadounidenses tienen una infinidad de herramientas y recursos, por eso son una alta potencia y existe una sección, una oficina. como es la CIA, tuve la oportunidad de ver un documental de de un de un de un informático que ahora que se hizo harker, en la cual él mismo hace referencia a cómo pueden obtener la información, de dónde se puede hacer una llamada incluso. Él. ¿Puede en ese momento que estamos hablando? ¿Puede aventarse mi teléfono? Y estar en la conversación que estamos nosotros, y grabarla y todo. Entonces siento que la la cooperación a nivel internacional y Estados Unidos es un país que colabora mucho. Pero pensaría, no sé, no sé, no sé cómo podría pensar si existe. Hay intereses de por medio que no se puede aplicar ese tipo de de colaboraciones, pero a nivel de ese tipo de delincuencias, de cómo cambia la forma de de investigar, cambiar la forma en quién son las personas que abocadas a la investigación de esa delincuencia, los recursos es importantísimo los recursos que puedo tener a la mano para poder, evidentemente. Obtener obviamente facilidad para investigar como son el reconocimiento de de de voz y cómo podría tener un la forma como ubicar a las personas que realizan las llamadas, entonces pienso yo que ese tipo de insumos podría ser una facilidad. Para poder establecer, obviamente. Una forma en cómo se podría identificar a las personas que son participes en ese tipo de delincuencia y pensando, por supuesto, en la colectividad. Aquí no estamos hablando de un interés personal, no lo hacemos que porque Jhonny es amigo mío, lo voy a hacer, oh porque Jordán es tuvo participación en ciertos, que no, aquí hay que pensar en la colectividad. En las personas ofendidas porque eso es lo que requiere un ofendido, yo voy a los estrados judiciales en la búsqueda por supuesto, de resarcimiento de un derecho, porque también el artículo 7 del Código Procesal Penal establece que. Hay que saber cómo se le puede restablecer los derechos de la víctima y pensar en la víctima es pensar, obviamente, en la

forma como se le puede dar. Correcta respuesta, como. Tiene el derecho a ser de informada, tiene derecho a que se le pueda resolver su su situación siempre, obviamente de una forma positiva. O por lo menos si no se pudo tener algo, pero se se se se abocó. OO se o. ¿Obtuvieron los recursos de investigación correcto idóneos para obviamente investigar esa delincuencia y eso no va a parar mientras no se apliquen métodos correctos de investigación en la forma cómo se estudia? ¿Esas delincuencias creo que las etapas van a seguir y van a seguir y van a seguir y esto? ¿A ser algo? Nunca acabar y al final de cuentas. Quien se llevara las decepciones son las víctimas porque sí me robaron todos mi esfuerzo de años y al final de cuentas fui al al Poder Judicial para que me resolvieran y no me resolvieron. Se abocaron a hacer nada más una diligencia o qué fui, pedí un levantamiento bancario, no hay nada. Entonces se archivó el expediente. Entonces la forma de investigar podría tener insumos positivos en el proceso, pensando siempre, obviamente proyectando los derechos de todas las partes del imputado. Que se le respeta usted de ellos, pero también era víctima que ha pedido auxilio judicial

Orador 1

Claro que sí, Don Jordán le agradezco mucho su tiempo y por ayudarme y colaborarme con esta entrevista.

Orador 2

Para mí ha sido un placer don Johnny, conozco su capacidad como profesional, Como estudiante también, en la cual espero que las intervenciones de este servidor hayan sido de Gran ayuda para su labor y también pensando en que esa situación también sea de una forma. ¿Cómo pueden ser observadas? Porque sé que esa tesis va a ser de utilidad y observación para fines académicos en la cual se pueda eventualmente, pues. Ser utilizado por algún alguna persona que pueda incluso incentivar en la Asamblea Legislativa para que pueda incluso cambiarse el sistema de investigación en ese tipo de delincuencias de acuerdo al conversatorio que hemos tenido tanto servicio como su persona. De igual forma agradecerle por pedirme la colaboración este gran proyecto que desde que lo comentamos. O usted me lo hizo ver, me llegó de tanta alegría porque es un tema muy interesante, pero lastimosamente. ¿Ha generado tantas dificultades en el entendido? El aspecto

judicial porque se ha o son desde decepciones para las víctimas que son o los ofendidos que son víctimas de ese tipo de delincuencias y en la cual pues se requiere algún tipo de auxilio por parte de la autoridad judiciales y en la cual pues seguir lastimosamente los métodos de investigación, pues no. O han o no han sido eficaces para la ubicación de esas personas que vemos que esto va en aumento, va aumento y lastimosamente pues no paran o no o no sea un aspecto positivo y esto la delincuencia lo ve como un como un halago para ellos, porque fue un reto adentrarse al sistema bancario para ultrajar las cuentas de las víctimas y ya lo ven como como algo tan satisfactorio para ellos y según las del mismo sistema, porque al final de cuentas se hacen pasar por funcionarios de prestigiosos bancos que ya incluso los bancos han perdido esa credibilidad. Le le agradezco que me haya tomado en cuenta y. Para servirle.

Orador 1

Claro que sí, muchas gracias don Jordán.

Orador 2

Que pasen muy bien, muy amable, bendiciones.

Fiscal Auxiliar MP

Archivo de audio

Audio entrevista Fiscal

Orador 1: Jhonny Rojas

Orador 2: Juez de Tribunal

Transcripción

Orador 1

¿Bueno, Buenos días, licenciado, ¿cómo está?

Orador 2

Muy bien y usted, don Johnny, un placer escucharlo.

Orador 1

Gracias bueno, para efectos de que conste en gradación mi nombre es Johnny Rojas, estudiante de la UIA. Maestría de Derecho Penal y para la misma, el marco metodológico propone una serie de entrevistas para recabar información para el tema de la tesis. El tema de la tesis Lic. Es “Los retos de la individualización de la persona autora del delito, estafa informática”. La misma la vamos a hacer a tipo de conversatorio con unas preguntas guía para mí, para ir encausando la conversación, entonces nuevamente le agradezco su anuencia y participación para conmigo.

Orador 2

Con mucho gusto la intención es colaborar y ayudar en lo que sería la mejora y la profesionalización de los de las distintas personas, en este caso usted en la Carrera de Derecho.

Orador 1

Muchas gracias, bueno, voy a iniciar Don Óscar, Don Óscar. ¿Cuál es su puesto dentro del Poder Judicial?

Orador 2

Actualmente tengo aproximadamente 6 años de estar destacando el puesto de fiscal.

Orador 1

Perfecto dentro del supuesto licenciado, posee experiencia en delitos de estafa informática.

Orador 2

En este caso, en el puesto que he estado destacando como fiscal auxiliar, si bien es cierto, no solo esos delitos he estado resolviendo, lo cierto del caso es que. Solo existe una Fiscalía especializada en San José, las distritales observamos todos los delitos, entre ellos observamos y resolvemos asuntos de estafas informáticas.

Orador 1

Perfecto OK dentro de las fiscalías distritales. ¿Qué tan común es atender este tipo de delitos de estafa informática?

Orador 2

En realidad, es bastante común porque se puede decir que todos los meses ingresan este tipo de denuncia. Las cuales inician en cualquier parte del país y en relación a la circular cero dos ADM 2019. Aunque la denuncia se reciba por ejemplo en Guanacaste, el expediente podría terminar de tramitarse en Limón. Esto por un tema de competencia, entonces, pese a los lugares donde se indiquen o se realizan las distintas denuncias, este no es necesario o no es exclusivo de esa Fiscalía que vaya a terminar resolviendo el asunto. Y de esa forma podríamos decir que hay un movimiento bastante fuerte y grosero en cuanto lo que sería los ingresos y movilidad de este tipo de delitos en toda en todas las fiscalías.

Orador 1

¿OK, entonces, dentro de su experiencia con su lapso de 6 años de laborar? ¿Cómo percibe usted el delito de estafa informática, si ha venido en aumentos o se ha mantenido? ¿Cómo lo cómo lo ves tú?

Orador 2

Sí considero que se ha estado dando un ligero aumento, el cual, si lo vemos por una cuestión porcentual, tomando en cuenta el crecimiento demográfico de los costarricense podríamos decir que porcentualmente se ha mantenido, pero numéricamente podríamos decir que sí ha aumentado el poco a poco al avanzar de los años.

Orador 1

¿Entonces sí podríamos hablar de que sí hay un aumento del mismo?

Orador 2

Exactamente.

Orador 1

Y licenciado. ¿Cuál es el medio más utilizado desde su experiencia que se utiliza para cometer este delito? Estafa informática, entiéndase llamada telefónica mensajes o páginas de Internet fraudulentas.

Orador 2

En realidad, considero y la mayoría de casos que he observado es por medio de la llamada telefónica, hablemos de la típica llamada de de la persona que dice que es del Banco que se va hacer Una transacción. Hablemos también de las llamadas de la municipalidad para pago de impuestos, otro ejemplo muy común es la persona que vende por Internet algún bien entonces pide que se le haga al simpe posterior a ello mencionan de que no sé lo que no ha llegado el dinero. Entonces hacen una supuesta llamada tripartita con un funcionario del Banco y ese es el típico o la forma más común en que se llega a observar este tipo de estafas.

Orador 1

Y considera desde su experiencia, que el delito Estado informática, en su mayoría se realiza de manera individual o una coautoría entre los delincuentes.

Orador 2

En realidad considero que es una coautoría, No obstante. En realidad, a final de cuentas, en en lo que sería la investigación, lo que logramos observar es que únicamente se logra determinar al dueño de la cuenta que recibe los dineros, el cuenta destino. Por temas de capacidad investigativa e inclusive por el modus operandi, estamos ante una situación que nos ponen en una dificultad

bastante amplia para poder ubicar al resto de personas, tómese en cuenta también principalmente en las llamadas tripartitas que estamos bajo supuesto de que se habla con una y con otra persona y al final de cuentas no tenemos certeza de quiénes son esas personas que realizaron las llamadas y al final de cuentas lo que logramos es ubicar al dueño de la cuenta receptor de los dineros fraudulentos.

Orador 1

Entiendo. Existe un procedimiento dentro del Ministerio público para los delitos estafa informática.

Orador 2

Podríamos decir que hay un procedimiento no escrito, dado que como toda investigación, hay ciertos parámetros que se llevan investigaciones. O cada investigación genera un tipo de diligencias particulares, principalmente al darse este tipo de delitos, con lo que son fraudes bancarios, el hecho de obtener la información bancaria de una persona y sustraer sus dineros. Básicamente lo que se genera principalmente son levantamientos de secreto bancario y posteriormente análisis de la información bancaria. A diferencia de otros delitos como los robos, como los homicidios, donde se pueden tener testigos que hayan visto los hechos y demás, este tipo de delitos tienen la particularidad de que casi toda la información analizar esa información escrita. Entonces se podría decir que sí hay una forma de trabajarlo, pero no es que exista un manual como tal, sino que la experiencia, el abordaje de cada caso nos va dando esa guía para poder lograr. Tratar de individualizar y eventualmente imputar a una persona.

Orador 1

Entiendo claro, dentro de la denuncia de la víctima. ¿Qué importancia o qué información es relevante de parte de la víctima para la identificación del delincuente que funcione para la identificación?

Orador 2

Para la identificación del delincuente. Básicamente, la información que él aborda es en cuanto a su propia cuenta. Lo que sería eventualmente el número de transacción para determinar cuál es la cuenta destino, y ahí es donde empezamos a tener, como le mencionaba anteriormente, la problemática de individualizar a otras personas, porque la información que nos logra brindar el ofendido va directamente en cuanto a las transacciones bancarias y el cuenta destino. En este caso, de forma evidente, el ofendido no ha logrado obtener información que nos permita de alguna manera individualizar a otras personas adicionales a cuenta destino.

Orador 1

Y eso es justamente el reto. Me imagino que dentro de la investigación se realiza como una pista, una huella tecnológica que es el reto a seguir por parte del Ministerio público.

Orador 2

Exacto, el reto es seguir acá. Se basa en dos situaciones. Primero, en cuanto a los números telefónicos, podría decirse que es sumamente fácil, eventualmente en cuanto a esa eventual huella de datos, poder hacer una verificación de radiobases una este un seguimiento de llamadas. Aló, aló, cierto, el caso es lo Que pasa Es que existen aplicaciones hoy en día que no permite. sí me escucha.

Orador 1

Sí como que se cortó un momento, pero ya. Estoy escuchando otra vez.

Orador 2

Sí, es que quiso entrar otra llamada. Este, como le explicaba en cuanto a las llamadas telefónicas. El problema es que existen aplicaciones que lo que hacen es disfrazar el número telefónico, inclusive se dan situaciones a donde se dan llamadas del extranjero, donde en este caso utilizan

este tipo de disfraces y ponen números telefónicos, indican los números de los distintos bancos haciendo creer al ofendido de una forma más fehaciente que lo están llamando exclusivamente. Del ente bancario donde tiene su dinero. Entonces, ese es el primer tema en en cuanto a lo que sería los números telefónicos en cuanto a los números telefónicos, la segunda circunstancia que pasa es el pobre control que tiene las distintas casas, Hablemos del ICE Kolbi, entre otros, y al momento de que una persona va y saca una línea telefónica, generalmente. Las los empleados, los subordinados. Con el fin de lograr esa venta y lograr una comisión, no registran debidamente, no verifican quiénes son las personas. Que se adjudican esas líneas y esos registros son sumamente endebles. Entonces no hay certeza de quién puede haber realizado la llamada o verificar si en realidad la llamada se dio desde el número telefónico o en su defecto de otro número con un disfraz. La otra parte que genera esa situación endeble de los seguimientos, porque. Desde. Aún. ¿Cómo le explico? Conjunto con las llamadas muchos momentos lo que hacen es enviar link por medio de correos para que las personas posteriormente ingresen sus datos, empezando todo por medio de una llamada telefónica. ¿Cuál es la situación existen? Buscadores en A nivel informático, como lo puede ser Tohr, como lo hay otros que utilizan lo que se llaman. Páginas o secuencias de búsqueda y pig.

Orador 1

Los que Camus, los que camuflan la IP.

Orador 2

Exacto, lo que llaman tipo cebolla. ¿Por qué se le por qué se le llama a este tipo? Porque la al igual que la cebolla, tienen capas entonces. Este tipo de buscadores, este tipo de programas, lo que hacen es utilizar y mandar primero la señal, no solo camuflando la IP, sino que además de eso hacen una línea de IP alrededor del mundo y genera tantas IP que no se logra llegar a la última. Y no solo es camuflar el IP igual como se hace con los teléfonos que es desplazarlo. Si no, lo que hacen es lanzan una IP de España que podéis pasar los datos, otra Inglaterra, otra Estados Unidos, otra El Salvador y luego llega a Costa Rica, pero las líneas que hacen este tipo de. Como le indico de coberturas de IP es tan Extenso que al momento de ir buscando. Una. Otra se llega a un callejón

sin salida, donde en algunas ocasiones regresan a una IP que ya había pasado anteriormente. Entonces, bajo esta situación es casi imposible lograr ubicar dónde está la computadora o cuál es el servicio de Internet. ¿De dónde salió esa esa información inicialmente? ¿Desde dónde se envió ese correo, ese link al correo? Los envíos. Entonces, toda esta situación es parte de la problemática para poder determinar e individualizar a las personas que están llamando a las personas que son los que están propiamente detrás de la estafa.

Orador 1

Y en un supuesto positivo de que supongo yo licenciado de que se logre determinar. El dueño de la IP existe bajo la premisa del derecho penal. Que es un que es personalísimo. ¿Cómo garantiza o cómo se garantiza que el dueño de la IP es el delincuente? Eso podría ser un reto.

Orador 2

Eso también sería eventualmente otro reto, dado que no sólo hay que verificar la IP como tal, habría que tener acceso a la computadora que utilizó la IP verificar cuáles son los márgenes De seguridad de esa máquina para garantizar si tiene clave si tiene usuarios. ¿Cómo determinar que solo la persona que se está tratando de imputar es la que utilizaba esa computadora y buscar ese parámetro? ¿Por qué? Básicamente tenemos la situación que en muchos casos en muchos hogares tienen una única computadora, la cual no tiene claves y un usuario y a la computadora tienen acceso 5 o 6 personas. ¿Entonces, bajo esa situación, o también dentro, la casi imposibilidad de lograr individualizar cuántas personas o qué persona es la que tenía acceso a esa computadora, y que en ese momento haya realizado la o que haya utilizado la computadora para enviar el link y realizar el de delito

Orador 1

Claro, eso es otro reto, por supuesto. ¿Licenciado, cómo es la colaboración para la obtención de pruebas por parte de los encargados de ciberseguridad de las entidades bancarias?

Orador 2

Ahí sí entramos en dos situaciones, la primera, en cuanto a la consulta como tal, considero que la colaboración como tal es buena desde puntos, desde el sentido de que siempre que haya una orden judicial y se haya llevado todo el proceso. Los distintos actos bancarios siempre nos contestan y nos envían la información. No se oponen. Cada vez que observan una resolución debidamente fundada y que realiza la orden y les envía toda la información que Ellos requieran Siempre nos contesta porque en realidad el problema no es la colaboración con los bancos, el problema es la capacidad que tienen los bancos para responder y eso sería el segundo punto que acá tenemos, que los bancos, a sabiendas de su obligación, tienen un personal para realizar dicha gestión. Es problema, es la demanda. Al existir tantas denuncias a nivel nacional. ¿Tantas solicitudes? Y ellos tengan un personal muy bajo para este tipo de funciones y lógicamente, desde el punto de vista comercial, al Banco no le va a servir tener 100 o 200 funcionarios sólo para esto, realizando una acción que evidentemente no le va a generar ingresos en su círculo comercial, sino únicamente gastos. La cantidad de personal que tiene es sumamente reducida. Por lo que genera que una respuesta de este tipo pueda durar año y medio a 2 años. Para ti propiamente, a la Fiscalía le llegue la información, esto pese a que se intenta realizar distintos recordatorios, sea mensuales. A los bancos para que nos envíen la información, he ahí donde está el verdadero problema de obtener la información que requerimos para poder seguir a las siguientes etapas.

Orador 1

Claro, es un plazo muy amplio el que tienen para Responder y por la materialidad del Banco de la capacidad, como dice usted, para poder dar esa información.

Orador 2

Exactamente, porque ahí no estamos ante una situación de. El Banco. Se esté negando o te está indicando que no lo va a hacer y tampoco es que se le otorga el plazo de año y medio. Años básicamente el Banco se le ordena que se le envíe la documentación y que ellos de inmediato

gestionen, pero vamos a la misma situación, es la gran cantidad de solicitudes que tienen. Aquí hasta donde tengo conocimiento, ellos los van organizando según a cómo van INGRESANDO y es ahí donde se da esta situación, aunado a que las órdenes también hacen ver que no solo tienen que mandar la información de la cuenta de destino, sino cualquier otra cuenta posterior a la que se haya enviado la el dinero. Por ejemplo, si la cuenta número 1 es la cuenta de los ofendido y se pasa el dinero a la cuenta dos, esa es la información que tenemos en El expediente. Pero una vez que los funcionarios bancarios revisan la cuenta dos pueden verificar que se pasó el dinero en la cuenta 3 a una cuenta 4, 5, 6, 7 y sucesivas, entonces todo lo que tienen que revisar y buscar, y toda la gran cantidad de información que nosotros pedimos, que generalmente tiene una información de un mes antes de la transacción, un mes después, quién es el historial de la cuenta? Quiénes son las personas que eventualmente este tenían acceso a esa cuenta y entre otra información más. Todo esto, ellos tienen que recabarlo y enviárnoslo a nosotros, y si eso lo hacen en cada caso. Y por la gran cantidad de información que se pide a nivel nacional, he ahí donde es entendible lo que duran los bancos en respondernos, pero desgraciadamente es. Esto genera una un retraso hacia los ofendido en un retraso a la justicia que evidentemente el Poder Judicial ni la Fiscalía tiene maneras de cómo solventar.

Orador 1

Por supuesto, varía en algo la misma anuencia colaborar en el caso de los proveedores de servicio de Internet o telefonía.

Orador 2

En cuanto a la recepción de información o devolución de información al Poder Judicial.

Orador 1

Exacto, vamos, cuando quiere investigar una IP o una llamada telefónica a través del número se le solicita, supongo yo que ya no al Banco, sino a la A la proveedora del servicio.

Orador 2

Sí, ese tipo de circunstancias en realidad. Muchísimo más rápido por lo general. Las distintas instituciones, como ICE, Movistar realmente. Lo que dura. Es aproximadamente tal vez 3 cuatro meses en estarnos contestando, porque esa información es o la información que se le solicita a ellos. ¿Es más simple? ¿Entonces, bajo esas circunstancias, es relativamente rápido tener esa información? En relación a otras diligencias, y lo que se aprovecha también en el tiempo, es que no solo se envía a ser una única diligencia, sino que se envían a ser diligencias a distintas instituciones o otras investigaciones al mismo tiempo para ir aprovechando los tiempos.

Orador 1

¿Claro licenciado, considera usted que a juicio o al proceso penal se logra llevar a los autores intelectuales del delito de estafa informática?

Orador 2

Por lo menos a mi consideración, considero que no, como se lo mencionaba al principio, generalmente se logra llevar a la persona en cuenta destino. Pero vamos esas circunstancias, no logramos tener, en cuanto al modus operandi, una certeza plena de que esa persona haya sido el actor intelectual. ¿Y al existir? Normalmente en las llamadas dos o 3 personas que llegan a conversar con el ofendido no podría tener certeza y por lo menos mi consideración es que no se logra llevar al actor intelectual. Esté a juicio en estos casos.

Orador 1

¿Entiendo y cuál es la posición de los imputados en cuanto a brindar información que permita identificar a otros autores O A un posible autor intelectual del delito de Estado informática?

Orador 2

Por lo menos hasta el momento, yo no he en ninguno de los casos que he tramitado, he tenido evidencia de parte de los imputados en indicar. Más bien siempre toman una posición de que no tenían mayor conocimiento de la situación, de que casi, que eso es un error y que lo que quieren es utilizar las distintas salidas alternas, como la conciliación, a efectos de buscar una reparación rápida del daño y evitar cualquier otra situación posterior, pero siempre. O en. Mayoría de las casas que he pedido se ponen en una posición de que básicamente ellos no tenían mayor conocimiento de la situación. Y que no saben. ¿Cuál es la persona que generó todas las circunstancias alrededor del delito?

Orador 1

¿otro reto más para el tema de los delitos de la individualización, verdad? ¿La falta de anuencia? ¿Cuáles son, considera usted licenciado? Son los principales obstáculos que dificultan la identificación del ciberdelincuente.

Orador 2

Los principales obstáculos, en realidad, nacen desde la posición de que tuvimos que recordar que no estamos en un país tercemundista, no estamos en un pais Que tengan. En este momento, la capacidad tecnológica para dar un seguimiento adecuado a todas las líneas electrónicas y demás gastos electrónicos que se dan alrededor de ese tipo de delitos. Entonces, si estamos en. Investigando estamos tratando de traer elementos probatorios, dentro de un asunto. Donde básicamente todo se da en relación a lo que tenían. Información electrónica. ¿Y si vemos a partir de eso que la investigación termina girando en relación a las información documental o la información electrónica que queda posterior al delito? Tenemos una gran falencia porque no logramos. Traer al proceso. Toda aquella situaciones relacionadas con propiamente el momento de la llamada, todo lo que tiene que ver con los envíos Y recepción de información en cuanto a correos electrónicos, a todas las todo lo que tiene que ver con los distintos parámetros de las IP. ¿Entonces, bajo esas circunstancias al poder judicial al No tener los medios económicos. Para de alguna manera traer el insumo. Tecnológico. A fin de dar este seguimiento, en realidad estamos ante una

falencia sumamente grave al no tener la capacidad de realizar una investigación acorde a la forma y los métodos del delito.

Orador 1

entiendo el Poder Judicial. ¿Está tomando alguna medida para superar esos desafíos que usted me comenta?

Orador 2

Hasta donde tengo encendido o por lo menos del conocimiento que tengo al respecto, sé que mi Poder Judicial no ha logrado por lo menos buscar la manera de darle ese tipo de seguimientos como le indico el problema mayor acá es un tema de capacidad económica para poder invertir en nuevas secciones dentro de lo que sería el OIJ y poder realizar este tipo de seguimiento.

Orador 1

Claro, entonces. Desde lo que usted me está partiendo indicando. ¿Usted podría identificar alguna tecnología o herramienta que considera que podría ser útil para mejorar la identificación del ciberdelincuente?

Orador 2

En este momento no preciso los nombres, pero sí existe lo que serían distintos programas. ¿Que permiten ese tipo de rastreos? Pero vamos a la misma circunstancias y. Tomando encuenta Inclusive en cuanto a lo que es la unidad de Cibercrimin, que cuenta con algunos programas para poder desbloquear teléfonos y otros afectos de descargar información. Hay que tomar En cuenta que todos este tipo de programas requieren licencias y esas licencias las tiene que estar pagando el estado a aquellas empresas que generan estos programas o aplicaciones, entonces ese Tipo de pagos, ese tipo de De información o programas que se tienen que generar. Por lo menos a nivel país. Creo que no tenemos todavía la capacidad ni el insumo humano para nosotros mismos, crear

ese tipo de programas a efectos de poder dar la trazabilidad de la información y ver dónde empiezan los puntos donde se da. Este los inicios de llamada o dónde están las computadoras por medio de las cuales se ingresa de forma violenta otras y tampoco se le está dando seguimiento, se está logrando comprar de ese tipo de software a efectos de poder dar de programas Al estado, al propio Poder Judicial y poder lograr de alguna manera este. Individualizar o llegarle a las personas que son las que inician este tipo de delitos.

Orador 1

¿Entiendo, claro, hablando un poquito de Cooperación Internacional, licenciado, entendiendo que el Convenio Budapest es como la principal herramienta en colaboración de ciberdelincuencia, considera usted? ¿Qué más se podría hacer a nivel de Cooperación Internacional para la identificación?

Orador 2

Bajo ese bajo esa posición prácticamente lo que podría incrementarse, primero tendría que abrirse una brecha un poco más amplia en cuanto. A lo que es la capacidad de información entre el organismo de investigación judicial y otros entes estatales de otros países. Para poder utilizar esa información, dado que por ejemplo, cuando se realiza algún tipo de Hablemos Comunicación entre países cuando tenemos que solicitar extradiciones o nacionalizar lo que sería prueba extranjera. ¿Todo esto tiene que pasar por medio de traducciones y demás, entonces todo ese tipo de trámites que llegan a ser un tanto? Complicados deberían buscarse cómo hacer cambios legislativos a efectos de simplificar y agilizar todos esos trámites. Dentro. La misma línea habría que buscar la manera de Estos estos otros países pudiesen colaborarnos con software que tengan que que permita este tipo de seguimientos, básicamente porque es la herramienta que necesitamos para poder. Llegar a este, a estas personas, a los actores intelectuales. Porque bajo la premisa que tenemos y el tipo de colaboración que se ha estado dando A final de cuentas. Y es muy fácil que quede en el papel algún tipo de colaboración y otra otra situación distinta es lo que logren hacer nuestros funcionarios desde aquí desde Costa Rica, porque es diferente, por lo menos a mi visión. De funcionarios de. Países extranjeros realizan algún tipo de. Acción, realizan algún tipo de

investigación y que no te equivoques. Podamos tener una mayor cantidad de mas pueba. Para. Realizar esto De búsquedas, tomando en cuenta también que hoy en día con lo que son las criptomonedas, entre otros. Muchos de los dineros. ¿Se llegan a terminar de destapar? A los ofendidos. Terminan en redes mundiales a través de este tipo de sistemas que evidentemente Costa Rica no tiene el medio para poderles dar seguimiento y tampoco se podría tener la certeza eventualmente si alguna persona traspasan los dineros a una cuenta de un sujeto y posteriormente desde esa cuenta realicen compras de criptomonedas posterior a ello, básicamente tendríamos. La pérdida completa de ese dinero porque no podríamos determinar a qué parte del mundo se fue y al En este sentido, al organismo de investigación judicial no tener las herramientas y depender de otros entes internacionales. Quedamos maniatados. Entonces, hasta que no se de ese apoyo que permita que el Poder Judicial desde el organismo de investigación judicial pueda darle ese seguimiento, básicamente vamos a seguir en la misma situación.

Orador 1

¿Qué recomendaciones generales? ¿Podría darme usted que se pueden mejorar para la identificación del ciberdelincuente?

Orador 2

En cuanto a recomendaciones como tal. En realidad es atacar el mismo problema. ¿Por qué Hasta que. Logremos sobrepasar la situación tecnológica que tengamos o que tenemos en este momento, no vamos a poder identificar debidamente estas personas porque sí tendríamos procesalmente hablando, lo que serían eventualmente los criterios de oportunidad tratar por medio de los de las personas que logramos individualizar, buscar la manera. Pero vamos a la misma situación, sabemos que los los imputados que logramos individualizar no nos están colaborando, requieren asumir ellos la carga penal y buscar medios. Para salir de aquellos casos que sí se denuncien, dado que lo único que tienen que realizar eventualmente su pago, dado que en cada 1 de estos procesos en interior directo de lo perdido es recuperar su dinero únicamente. No le interesa el seguimiento de una causa y poder determinar quiénes son las personas. ¿Que cometieron el delito y quién es? Actor intelectual. Entonces lo que tenemos que abocarnos es a buscar herramientas que nos permitan en

realidad. Dar un seguimiento o llamémosle electrónico, un seguimiento de. En cuanto a la movilidad de datos en Internet y otras redes. Para tratar de llegarle a esas personas. Y para eso lo que necesitamos es un soporte hardware, perdón, de software. Que nos permita. En este caso, llegarle a esas personas, modificar de dónde vienen esa información y poder llegarle a esos domicilios. Individualizar. Es por ahí donde tenemos que empezar hasta que no logremos superar esa brecha tecnológica. A mi consideración no vamos a tener. Una forma efectiva de poder llegar a estos a los actores indelectuales. Todos estos delitos.

Orador 1

Nomás que le agradezco mucho su tiempo y la información brindada ha sido muy enriquecedora y muy provechosa.

Orador 2

Con muchísimo gusto y la intención siempre es de mi punto de vista, tratar. Expandir el conocimiento y que en este tipo de charlas y de igual manera, poco conocimiento que cada persona o mucho conocimiento que cada persona también pueda tener este irlo repartiendo. Tratar de hacer mesas de diálogo, buscar soluciones y de esta manera. Mejorar tanto el procedimiento penal, que es la carrera que. En este caso. Aborda o yo en cuanto a mi carrera de Derecho y mi especialidad en Derecho penal. En usted de esta manera, todo lo que sería mejorar los distintos procedimientos y lograr hacer que estas personas que cometen algún tipo de delito. Vengan y lograr hacer que pague, por decirlo. ¿Alguna manera? Todos esos tipos de opciones y resarcir de alguna forma los ofendidos en cada uno de los procesos.

Orador 1

Así es, muchas gracias de verdad.

Orador 2

Con mucho gusto.

Cuestionario de Fiscala

1. ¿Cuál es su puesto dentro del Poder Judicial?

R/ Fiscal Coordinadora

2. ¿Posee experiencia en delitos de estafa informática?

R/ Si

3. ¿Qué tan común es atender delitos de estafa informática?

R/ Aproximadamente de tres a cinco causas mensuales por cada Fiscal Auxiliar

4. ¿La estafa informática ha venido en aumento?

R/ Si, con el desarrollo tecnológico, la facilidad de adquirir teléfonos celulares, líneas telefónicas y acceder a plataformas digitales, redes sociales, propicia canales aptos para este tipo de criminalidad.

5. ¿Cuál es el medio más utilizado para cometer el delito de estafa informática? (-llamada telefónica, mensajes, páginas de internet)

R/ Llamadas telefónicas, donde las personas mediante un ardid del interlocutor

6. ¿El delito de estafa informática en su mayoría, se realiza de manera individual o en coautoría por los delincuentes?

R/ Este tipo delitos, son ejecutados mediante criminalidad organizada, donde personas que difícilmente se logren identificar, manipulan los sistemas informáticos, en la mayoría de los casos desde direcciones IP, ubicadas fuera de nuestro país, quienes en conjunto con los titulares de

cuentas bancarias, utilizando sus cuentas bancarias como fuente receptora de los fondos transferidos ilícitamente.

7. ¿Cuál es el tipo de estafa informática más frecuente en Costa Rica? (–ingeniería social, Phishing, Malware-)

R/ Phishing

8. ¿Existe un procedimiento en el MP para los delitos de estafa informática?

R/ Se recibe la denuncia del ofendido, solicitud de levantamiento de secreto bancario, identificación de los imputados, decomiso de videos de seguridad de los cajeros automáticos o de ventanillas bancarias, decomiso de documentación y de ser posible análisis grafoscópicos. Generalmente se logra identificar únicamente a los sujetos que realizan los retiros de dinero,

9. ¿Qué información es relevante por parte de la víctima para la identificación del delincuente de estafa informática?

R/ Usualmente los delincuentes son desconocidos para la víctima.

10. ¿Cómo es la colaboración para la obtención de pruebas por parte de los encargados de ciberseguridad de las entidades bancarias?

R/ Siempre remiten los solicitado, sin embargo el tiempo de entrega es prolongado debido a que es una sola oficina en cada banco que se encarga de recabar dicha información.

11. ¿Considera usted que a juicio se logra llevar a los autores intelectuales del delito de estafa informática¨?

R/ No, generalmente se logra identificar y vincular a los receptores del dinero.

12. ¿Cuál es la posición de los imputados en cuanto a brindar información que permita identificar al autor intelectual del delito de estafa informática?

R/ En mi experiencia nunca han brindado ese tipo de información, lo que declaran frecuentemente es que prestaron la cuenta a algún conocido.

13. ¿Cuáles considera usted son los principales obstáculos que dificultan la identificación del ciberdelincuente?

R/ Generalmente los sujetos que manipulan los sistemas informáticos están fuera de nuestro país.

14. ¿Qué medidas se están tomando para superar estos desafíos?

R/ Considero que son escasas las herramientas con las que contamos actualmente y pocos los esfuerzos para mejorar.

15. ¿Qué tecnologías o herramientas considera que podrían ser útiles para mejorar la identificación del ciberdelincuente?

R/ Mejor comunicación internacional para ubicar las direcciones IP desde donde se realizan las transacciones fraudulentas.

16. ¿Qué medidas de cooperación internacional considera necesarias para mejorar la identificación del ciberdelincuente?

R/ El Ministerio Público cuenta con una oficina encargada de las coordinaciones internacionales y que necesita recurso para incrementar esfuerzos y crear vínculos con otros Ministerios Públicos extranjeros.

17. ¿Qué recomendaciones generales tiene para mejorar la identificación del ciberdelincuente?

R/ Ese tipo de investigaciones requiere de un recurso humano capacitado en ingeniería informática con entrenamiento forense, debido a que los abogados carecemos de ese tipo de conocimiento.

Buenas tardes, espero que haya sido de ayuda. Si necesitas que amplíe mis respuestas, quedo atenta.

Saludos cordiales;