El fraude electrónico

Electronic fraud[1]

Resumen

El fraude electrónico es un problema muy serio que perjudica a sus víctimas de una forma grave. Al analizar la estructura del delito del fraude electrónico, se identifica que este se consuma desde el momento en que la entidad financiera aprueba la transferencia y una vez hecha es muy difícil revertirla, porque el dinero fue transferido electrónicamente a otra cuenta. Este tipo de delito va en aumento y las autoridades judiciales deben prepararse para frenar el crecimiento de estos hechos delictivos y evitar que queden impunes. Debido a que las entidades financieras han adoptado medidas de seguridad cada vez más fuertes, los criminales se las han ingeniado para bordear esa barrera de seguridad que se ha implementado. Por esto es necesario crear un sistema que sea lo suficientemente moderno y eficiente para rastrear y ubicar al criminal de una forma fácil y rápida, y para entender mejor esta problemática tan ingeniosa, pero dañina para la sociedad, se abordan conceptos muy importantes para el tema en investigación, así como datos relacionados con cada tipo de fraude en cuestión, además del análisis de posibles soluciones al problema.

Palabras clave: Fraude, suplantación de identidad, secuestro de datos, víctima, banca electrónica.

Abstract

Electronic fraud is a very serious problem that harms its victims in a serious way. When analyzing the structure of the crime of electronic fraud, it can be identified that it is consumed from the moment the financial institution approves the transfer and once it is made, it is very difficult to reverse it because the money was transferred electronically to another account. This type of crime is on the rise and the judicial authorities must prepare themselves to be able to stop the growth of these criminal acts and prevent them from going unpunished. It has evolved and because financial institutions have adopted increasingly strong security measures, criminals have managed to get around that security barrier that has been implemented. For this reason, it is necessary to create a system that is modern and efficient enough to track and locate the criminal in an easier and faster way and to better understand this problem that is so ingenious but harmful to society, very important concepts are addressed for the topic in question. investigation, as well as data related to each type of fraud in question, in addition to the analysis of possible solutions to the problem.

[1] Jordan Steven Benavides Blackwood, estudiante de Licenciatura en Derecho. ULACIT. Correo Electrónico: jbenavidesb@ulacit.ed.cr

Keywords: Fraud, phishing, ransomware, victim, e-banking.

Introducción

El presente trabajo aborda el tema del fraude electrónico desde una perspectiva unificada, con los aspectos más relevantes sobre conceptos, ejemplos, noticias, legislación nacional, derecho comparado, origen del problema y recomendaciones hechas por expertos en la materia para disminuir la cantidad de víctimas de este delito informático.

El tema del fraude electrónico es un problema muy serio, que perjudica a sus víctimas y que está presente en varios países de la región. A este respecto, Gabaldón (2006) señala que "el desarrollo de las tecnologías de la información puede favorecer de varios modos el desarrollo de los fraudes, como una actividad colateral de la expansión de la movilización del dinero" (p. 197). Es por esta razón que las autoridades deben avanzar y estar a la vanguardia ante los nuevos métodos de fraude que se dan actualmente, pues de otra forma la población estaría muy expuesta a este tipo de amenaza invisible que causa grandes pérdidas económicas a sus víctimas.

El fraude electrónico va en aumento y las autoridades judiciales deben prepararse para frenar el crecimiento de estos hechos delictivos y evitar que queden impunes. De acuerdo con Castro (2021), "en términos generales la Fiscalía Adjunta de Fraudes y Cibercrimen percibió un aumento desmedido en el uso de los sistemas de cómputo, redes sociales, páginas web y gemeleo de medios electrónicos, producto del confinamiento por la pandemia" (p. 1); y por esta razón, es necesario crear un sistema que sea lo suficientemente moderno y eficiente para rastrear y ubicar al criminal de una forma fácil y rápida. Para entender mejor esta problemática tan ingeniosa, pero dañina para la sociedad, se abordan a continuación conceptos muy importantes para el tema en investigación, así como datos relacionados con cada tipo de fraude, con una reseña histórica.

Metodología

Se realizó una investigación sobre el fraude electrónico desde una óptica de análisis de los conceptos informáticos; datos históricos; situación de las víctimas de este delito; cómo se pudo haber prevenido; qué se puede hacer para que no se vuelva a repetir; reparación del daño sufrido; y determinar, mediante el derecho comparado desde la óptica de Costa Rica, soluciones que otros países de la región han adoptado para disminuir el incremento en la incidencia de estos casos que perjudican económicamente a las personas víctimas. Es un problema que crece cada año y se deben tomar las medidas correctivas, punitivas y preventivas para erradicar este mal que tanto preocupa a la población costarricense.

Reseña histórica

Aunque se piensa que este tipo de delito es muy reciente o novedoso, la historia demuestra que no es así, pues al igual que "las computadoras que evolucionaron desde la primera hasta la octava generación que son las computadoras del año 2011 en adelante" (Hernández, s. f., p. 1), lo mismo ha sucedido con este delito que con el pasar de los años ha llegado a un punto que se considera está muy avanzado. A este respecto, Sain (s. f.) señala que

> a partir de los primeros años de la década de 1980, los delitos informáticos adquieren una importante notoriedad a partir de un aumento exponencial de fraudes y el tratamiento de la problemática por parte de organismos internacionales. Para el caso de los fraudes, los casos típicos se realizaban mediante la manipulación de uso de tarjetas de débito en cajeros automáticos, fundamentalmente a través de la vulneración de las bandas magnéticas. Esto motivó la utilización por parte de las empresas emisores de la adopción de chips en los plásticos como medida de seguridad (p. 3).

Los fraudes electrónicos han venido evolucionando y debido a que las entidades financieras han adoptado medidas de seguridad cada vez más fuertes, los criminales se las han ingeniado para bordear esa barrera de seguridad que se ha implementado; por ejemplo, si un banco tiene medidas de seguridad muy rigurosas que protegen el dinero, el criminal tiene que obtener el acceso para poder abrir esa barrera casi impenetrable, por lo que entra en juego el tema de la ingeniería social, que tiene como objetivo brincarse esa seguridad haciéndose pasar por el cliente, por lo tanto ante una situación así, el sistema informático del banco o entidad financiera no tiene forma de saber si quien ingresa a sus sistemas con un usuario y contraseña debidamente registrados es verdaderamente el dueño de esos datos o no, como en un caso de robo de datos o suplantación de identidad. Es en este punto donde se está actualmente, porque el fraude electrónico ha avanzado de ser un fraude hecho para engañar sistemas de seguridad débiles como en los años noventa, vulnerando bandas electromagnéticas, a ser un fraude hecho para engañar a los dueños de esas contraseñas que dan el acceso a estas cuentas bancarias con barreras de seguridad casi impenetrables.

Se debe hacer conciencia sobre los peligros del internet y los celulares y demás dispositivos electrónicos que acceden a estos sistemas bancarios, siempre se debe desconfiar de personas desconocidas —o conocidas— que nos pidan información

privada, como las contraseñas y usuarios de plataformas web o aplicaciones de bancos que permiten realizar transacciones a otras personas mediante una simple o varias transferencias electrónicas; actualmente hasta una transferencia vía sinpe móvil que

> se dirige al segmento de pagos al detalle (de bajo monto), para que los usuarios del Sistema Financiero Nacional puedan realizar transferencias electrónicas de dinero a cuentas vinculadas a números de teléfono móviles, desde cualquier canal de banca electrónica (Banca SMS, Banca Web Móvil, Banca App, Banca en Línea o Red de Cajeros Automáticos) (Banco Central de Costa Rica, 2022, párr. 1).

Entonces, cabe mencionar que, para el caso del fraude electrónico actual, los usuarios de estos sistemas no deben preocuparse por la seguridad misma del sistema, sino más bien en que nadie obtenga el acceso a esas contraseñas que al final de cuentas es el modo con el que los criminales acceden al dinero.

Por otra parte, este problema que crece diariamente parece no tener solución y que no se puede hacer nada al respecto, y es que los bancos culpan a sus clientes por no cuidar sus datos personales, como lo menciona Díaz (2022):

> ¿Cuán responsables son los bancos por la duplicación de los sitios web, el uso de teléfonos oficiales de sus oficinas y otras estrategias que los clientes no conocen bien?
>
> Distintas víctimas relataron que, ante la suplantación de correos oficiales del Nacional, reciben como respuesta: “Es una estafa, pero si usted brinda sus datos privados a terceros, el banco no se responsabiliza” (párrs. 3-4).

Las entidades bancarias no toman en cuenta que las víctimas son engañadas mediante la “ingeniería social” que consiste en

> el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan

> entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo (Sandoval, 2011, párr. 5).

Otra definición muy específica en cuanto al *modus operandi* es la actuación "directamente sobre la víctima manipulándola psicológicamente mediante el engaño, para que comparta información confidencial (credenciales de acceso, nombres de usuario, contraseñas, etc.) o realice acciones inseguras (ejecución de algún archivo o deshabilitación de alguna función)" (García, s. f., p. 5).

En estos casos, cabe mencionar que las personas víctimas de esta maniobra que ejecutan los perpetradores no saben lo que están haciendo, pues están confiando en otra persona, que supuestamente les ayuda a solventar un problema ficticio de seguridad en la cuenta, ante lo cual la víctima da toda la información confidencial pensando que quien está al otro lado del dispositivo es un representante real de la entidad financiera que tiene como objetivo resguardar el dinero que tiene en su cuenta. Este es un acto de engaño que ocurre muy rápido, todo es en tiempo real; la víctima —al confiar— no toma ninguna medida de prevención, debido a que supuestamente le están ayudando de acuerdo con lo que le diga el perpetrador, ya sea para proteger la cuenta aumentando la seguridad o recuperando un dinero producto de una transacción que en la realidad nunca ocurrió.

En la mayoría de los casos, cuando la víctima se percata de que lo vivido no coincide con la realidad o algo no anda bien, llaman al banco o entidad financiera para confirmar lo realizado y es en ese momento cuando reciben la noticia de que fueron víctimas del fraude electrónico. Para entonces, ya es demasiado tarde, ya ha sufrido el fraude y el dinero ya fue extraído de la(s) respectiva(s) cuenta(s) bancaria(s).

De acuerdo con Marín (2022), una encuesta publicada por la UCR muestra que "un tercio de los hogares del país ha sufrido estafa o intento de estafa por medios digitales desde que inició la pandemia" (párr. 1). Además, "muestra un resultado señalando entre los encuestados que «el 26.3% experimentó algún intento de estafa y el 4.9% señaló que algún miembro de su hogar fue estafado por estas vías»" (párr. 5). Como se puede apreciar, es impresionante el grado de facilidad que tienen los delincuentes para cometer estos delitos, y no importa el lugar en donde estos se encuentren, pues con una llamada telefónica es suficiente para cometer el ilícito, y la persona que contesta la llamada, sin ser consciente de la magnitud y relevancia del

simple hecho de hablar con un desconocido para brindarle información que no debe dar, se convierte en una nueva víctima de este tipo de delito.

El fraude electrónico engloba varias formas de ideación y realización que materializa el perjuicio económico a sus víctimas, entre estas formas complejas de engaño están las siguientes:

El *phishing* y el *pharming,* que tienen como fin

> apoderarse de información personal de un usuario de internet, para acceder a sus cuentas de correo o de redes sociales y obtener adicionalmente datos de sus contactos virtuales, a fin de comerciarlos ilícitamente, o bien, conseguir claves de "e-banking" para de este modo ingresar a las cuentas corrientes bancarias de los titulares y disponer del dinero que en ellas se encuentra, realizando una operación de transferencia de activos a un tercero que se denomina "mule" (en adelante, mulero o mula) (Oxman, 2013, p. 215).

El *phishing*

> es la pesca de datos personales a través de Internet. Ahora bien, ella puede constituir una modalidad de estafa informática, si tiene lugar a través del envío masivo de correos electrónicos con enlaces a páginas web falsas, respecto de las cuales se imita el contenido o la imagen de una determinada entidad financiera o bancaria para engañar al destinatario del mensaje, logrando así sustraer información personal que posibilita el acceso a sus cuentas de débito personal (Oxman, 2013, p. 217).

El *pharming* consiste en

> la manipulación técnica de las direcciones DNS que son utilizadas por un determinado usuario, reconduciendo la navegación que este realiza a

> sitios web que presentan un aspecto idéntico, pero que son falsos y han sido creados con fines defraudatorios. Esta figura puede operar como modalidad de estafa informática si con el mecanismo indicado se consigue la cesión de datos personales financieros o bancarios, con el propósito ulterior de realización de ilícitos de apoderamiento patrimonial de dinero o activos en cuentas corrientes (Oxman, 2013, p. 217).

También existe el *spyware*, que "son aplicaciones o programas que se instauran en el sistema, generalmente con el propósito de recopilar información del usuario almacenada en el sistema informático sin su autorización; esta información es enviada al desarrollador del spyware generalmente para usos publicitarios" (García, s. f., p. 3).

El *ransomware*

> es una aplicación que retiene o secuestra la información del usuario (a través de algoritmos de cifrado de datos) o realiza restricciones al sistema, (inhabilitando el sistema informático) para luego solicitar al usuario un pago económico (rescate de la información o habilitar el sistema informático) (García, s. f., p. 4).

Este software es tan avanzado que se podría pensar que se comporta de una forma autónoma; es tan maligno que una vez cifrada la información no hay manera de recuperarla y en muchos casos se da por perdida, debido a que, aunque se realice el pago del rescate de la información, esto no garantiza su recuperación total. Por esta razón, el *ransomware* es tan dañino y debido a esto se recomienda hacer copias de seguridad del sistema operativos y de los datos que se almacenan en este.

Por otra parte, en los casos de llamadas telefónicas para cometer estafas electrónicas, sería más fácil la ubicación de los perpetradores por medio de la tecnología de ubicación celular por triangulación, que

> consiste en captar la señal que emite el teléfono móvil que se desea localizar mediante una antena direccional para conocer la dirección en

> la que se encuentra más no la distancia. Para ello se emplea una segunda antena direccional ubicada a una distancia conocida de la primera antena. Dicha antena determina de nuevo la dirección relativa sobre la que se encuentra el punto a localizar. Conociendo las dos direcciones relativas a ambas antenas se trazan dos segmentos de recta, antena-celular de tal forma que en la intersección de ellas se ubicará al equipo celular. El rango de precisión en la ubicación del equipo está entre 50m a 200m (Silva, 2016, p. 3).

Con la ayuda de esta forma de localización, las autoridades logran ubicar y judicializar a los criminales.

En la actualidad, es necesario protegerse muy bien de los cibercriminales, se recomienda tener mucha precaución al respecto, los noticieros inundan a la población con testimonios de víctimas para que se haga conciencia y se evite caer en estos engaños, pero como señalan Santillán y Becerril (2009),

> lamentablemente, como todas las áreas de rápido crecimiento y pronunciado interés en la población en general, estamos propensos a ataques por parte de maleantes. Nuestra información financiera es muy valiosa, ya sea para que alguien realice una compra con nuestra tarjeta, o para utilizarla como identificación para procesos más complicados (y, usualmente, mucho más nefastos) (, párr. 2).

Es por esto por lo que se debe ser muy cauteloso con quien se habla y se brinda información sensible y no se debe confiar cuando nos den datos confidenciales obtenidos ilícitamente para tratar de ganar nuestra confianza mediane llamadas telefónicas o donde se navega con ordenadores y se va dejando información financiera que al final de cuentas es el objetivo de los cibercriminales para obtener el beneficio económico.

Pero los atacantes no se conforman solamente con obtener la confianza de sus potenciales víctimas, sino que además de esto se fían de herramientas tecnológicas para los casos de la obtención de información financiera, y es que “los atacantes tienen una

amplia gama de opciones para obtener nuestra información. Se valen de engaños (phishing, pharming), espían nuestras actividades (spyware) y, en algunos casos incluso nos atacan directamente (gusanos, virus) con tal de conseguir lo que buscan." (Santillán, Becerril, 2009, pág.1)

Como se puede apreciar anteriormente, las personas que se dedican a realizar estos hechos criminales no son inexpertos, porque en la mayoría de los casos cuentan con conocimientos en informática, ya saben cómo actuar con tal de conseguir el objetivo principal, que consiste en obtener la información de

> Los números de tarjeta de crédito (en conjunto con la información periférica necesaria, como el código de 4 dígitos adicional) que permiten a los maleantes realizar cargos a nuestro nombre, no solo para adquirir mercancías, sino también para suplantar nuestra identidad a la hora de registrarse en algún sitio u organización. (…) En segundo lugar los maleantes buscan hacerse de la información que da acceso a los sistemas de banca electrónica; esto es, nuestros nombres de usuario y contraseñas. (Santillán, Becerril, 2009, pág.2)

Ante esta situación, algunas entidades financieras han adoptado medidas para proteger a sus clientes, lo cual es de suma importancia tomando en cuenta que muchos clientes no poseen conocimientos básicos sobre el funcionamiento de la informática y son blanco fácil de los cibercriminales, por esta y otras razones

> hasta hace un año, existen seguros (para cubrir parte del dinero perdido) en dos bancos, BAC con una aseguradora privada y Banco Popular con el Instituto Nacional de Seguros. Si vas al Banco Nacional, no existe. En el BCR tampoco. Cooperativas y mutuales menos", explicó la abogada Adriana Rojas, especialista en derechos de consumidores bancarios y quien defiende estafas desde el 2008 (Díaz, 2022, párr. 19).

Es de suma importancia que las entidades financieras tomen conciencia de que si el cliente es estafado, este espera una respuesta positiva de su banco, que debe saber responder ante un caso de fraude electrónico, y es que si el cliente no sabe qué hacer

ante un hecho de tal magnitud, en buena teoría se espera que el banco haga algo al respecto, y si la operación financiera producto del fraude no se puede revertir, al menos el banco debe brindar un seguro antifraudes que proteja a sus clientes.

Ahora bien, con respecto al seguro antifraudes, como bien lo indica Díaz (2022), este solo repone una parte del dinero defraudado, por lo que esta es una situación que genera un sentimiento de desamparo en las víctimas ante estos hechos, en los cuales, en la mayoría de los casos, los bancos no saben cómo recuperar el dinero sustraído y lo dan por perdido, por lo que se utiliza la póliza de seguro, si existiere, porque como se pudo ver, no todos los bancos tienen esta medida de seguridad de seguro antifraude.

Por otra parte, en cuanto a la seguridad jurídica, el fraude electrónico se encuentra tipificado en el ordenamiento jurídico costarricense, específicamente en el Código Penal, con el nombre de "estafa informática" (Asamblea Legislativa de la República de Costa Rica, 1970), lo cual es muy importante para que el Estado pueda ejercer el poder punitivo en contra de los actores de estos delitos. Como se puede apreciar, este delito se tipifica con el sinónimo equivalente a fraude electrónico, pero de una forma más amplia, lo cual no perjudica su tipicidad por un mero hecho de nomenclatura, pues al final de cuentas, para un juez penal, tienen el mismo significado, de acuerdo con diccionarios de la lengua española en cuanto al uso de las palabras "fraude" y "estafa" en relación con los hechos criminales objeto de la investigación; por ejemplo, para la RAE, en cuanto a su definición oficial, el fraude es una "acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete" (Real Academia Española, 2022); y la estafa es el "delito consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro" (Real Academia Española, 2022).

En cuanto al análisis de las dos definiciones anteriores, con respecto a la tipicidad, para llevar a cabo la estafa se necesita realizar primero el fraude, que consiste en el engaño mediante acciones contrarias a la verdad, porque la estafa necesita del elemento del engaño, el cual configura el fraude, por lo que es requisito para cometer el ilícito penal.

Por otra parte, con respecto a la palabras 'electrónica', esta consiste en la "parte de la física que estudia los cambios y los movimientos de los electrones libres y la acción de las fuerzas electromagnéticas y los utiliza en aparatos que reciben y transmiten información" (Dictionary.com, 2022); y la informática es un "conjunto de conocimientos técnicos que se ocupan del tratamiento automático de la información por medio de computadoras" (Dictionary.com, 2022).

De acuerdo con las anteriores definiciones, se podría inferir que la informática actualmente necesita de la electricidad para funcionar, pero no se sabe cómo será el futuro en cuanto a la fuente de energía de estos dispositivos, y el legislador optó por la palabra que más se adecúa a un posible cambio que afectaría eventualmente la tipicidad

en el futuro, para evitar así una posible reforma legal ante una eventual inseguridad jurídica.

Como se mencionó anteriormente, se puede observar que la legislación actual es robusta y trata de abarcar todo lo posible en cuanto a este tipo de hechos delictivos, en cuanto al castigo punitivo hay diferencia con otro tipo penal casi de mismo nombre, solamente omitiendo la palabra informática, pero en cuanto a la ideación del delito es incluso muy similar, se refiere a la sanción del delito de "estafa" (Asamblea Legislativa de la República de Costa Rica, 1970) regulado en el mismo código. Cabe mencionar que la diferencia entre ambos tipos penales radica en los medios para, en el presente caso, el uso de las tecnologías de la información.

Entonces si se posee con una legislación apropiada, se podría preguntar si el gobierno tiene las herramientas adecuadas y los recursos necesarios para perseguir estos delitos, y es que los problemas de persecución de estos hechos delictivos son muy complejos; a continuación, se mostrará una lista de obstáculos que deben afrontar los investigadores de las autoridades cuando se enfrentan a estos delitos.

Ante los problemas de persecución, es necesario mencionar que "este tipo de infracciones 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" (Acurio, s. f., pág. 55). En el caso de Costa Rica, ya existe un colapso judicial, tal como lo mención Díaz (2022), cuando entrevista al jefe de fraudes del OIJ, Yorkssan Carvajal, quien menciona el colapso que actualmente sufre el OIJ para resolver estos delitos:

> "En efecto, el OIJ está colapsado, eso no es un secreto para nadie. El año pasado, en ingeniería social, que es fraude informático, nos entraron 3.179 denuncias. Este año, en general, el primer trimestre de todas las estafas vamos con 2.600. Son datos bastante alarmantes que hace que entremos en un colapso de investigación porque la carga laboral de cada investigador es altísima con tantas denuncias de que los costarricenses, lamentablemente caen en estas estafas", afirmó Carvajal (párr. 18).

Para solventar este problema, es necesario que el gobierno invierta más recursos para que los investigadores tengan la capacidad de afrontar esta situación tan preocupante para muchos costarricenses. Una mejor manera de abordar estos casos sería cuando

> se formen unidades Investigativas tanto policiales como del Ministerio Público especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. Lo cual es posible aplicando la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos. (Acurio, s. f., p. 54).

Estas unidades investigativas tendrían como objetivo el reforzamiento de la investigación normal que realiza el Ministerio Público; serían unidades especializadas en la persecución de estos hechos de una forma exclusiva y sin precedentes, lo cual vendría a beneficiar al sistema judicial aumentando su capacidad de respuesta. Es fundamental que un país tenga la capacidad punitiva suficiente para que los criminales se hagan responsables de sus hechos, y se logre disminuir la impunidad, que en estos casos es muy alta. Una unidad especial mediante la cooperación internacional lograría llevar a cabo sus tareas investigativas de una forma más rápida y eficiente.

El fraude electrónico es un delito informático que se subdivide en distintas modalidades de ejecución, y para entenderlas es necesario saber cuáles son y su definición:

> 1. Los datos falsos o engañosos: (…) Conocido también como manipulación de datos de entrada.
>
> 2. Manipulación de programas o los caballos de troya: (…) Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.
>
> 3. La técnica del salami: (…) Consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

4. Falsificaciones informáticas: (…) Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original.

5. Manipulación de datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático.

6. Phishing: Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo (Acurio, s. f., pág. 23).

Las anteriores definiciones son una pequeña muestra del nivel de tecnología que pueden emplear los cibercriminales para realizar estos fraudes, son delincuentes sin escrúpulo en cuanto al grave daño que causan. A diferencia del fraude en su esencia original, el fraude electrónico de hace valer de herramientas tecnológicas y metodologías muy novedosas que evolucionan con el tiempo, y que como consecuencia del medio idóneo —en este caso la tecnología— logran su objetivo principal, que consiste en el perjuicio patrimonial de la víctima.

Es común ver artículos y noticias sobre el mundo de la tecnología que les recomiendan a las personas tener un sistema antivirus de buena calidad, pero de qué sirve tener un buen antivirus si las personas brindan su información a quien no deben, porque claro que un buen sistema antivirus puede ayudar a mejorar la seguridad del computador; sin embargo, hay que recordar que el antivirus es un software que ayuda a combatir otros tipos de software maliciosos, que tienen como objetivo la extracción de información confidencial como la de las tarjetas de crédito o claves de acceso almacenadas en el ordenador, pero poco podría hacer el antivirus ante situaciones donde las víctimas sin la pericia necesaria introducen sus datos personales en sitios web o programas donde no deberían.

Ahora bien, cabe mencionar que no todo está perdido en cuanto a la lucha contra el cibercrimen, por ejemplo, ya varios países han adoptado medidas importantes para reducir la incidencia de estos hechos. A continuación, se verá cómo otros países de la región han adoptado medidas para solucionar este problema.

Colombia: En cuanto al país colombiano, se debe reconocer que su gobierno ha implementado soluciones tecnológicas para la prevención de fraude, como el caso del

análisis de información, lo cual es una medida muy efectiva para el análisis de estos delitos y su mitigación, tal como comentan Moreno *et al.* (2019):

> Se han desarrollado sistemas de monitoreo y control que facilitan el levantamiento de información relacionada con las transacciones a través de los medios electrónicos. Estos sistemas realizan el análisis de diferentes factores relacionados tanto con los procesos de acceso y la actividad que se realiza en las diferentes plataformas, como de los dispositivos desde los cuales se realizan estos trámites, buscando detectar acciones no habituales (p. 38).

Este sistema de seguridad es muy innovador y eficiente, al tratarse de una medida de seguridad automatizada, en beneficio de los clientes bancarios que utilizan sus plataformas para realizar transferencias electrónicas. Es un ejemplo de una solución preventiva muy efectiva. Ahora bien, en el caso de América Central, el país vecino de Costa Rica al sur también tiene un sistema innovador desde el punto de vista de la investigación del delito con efecto intimidante para los delincuentes, a diferencia del modelo colombiano que se enfoca en la prevención.

Panamá: En el plano de la realidad del país panameño, este ha implementado medidas de ciberseguridad muy buenas, se debe reconocer que este país ha mejorado mucho su seguridad en los años recientes, a pesar de una regulación básica y es que

> Panamá, da sus primeros pasos en la búsqueda de mitigar los delitos informáticos, bajo la estructura de la Autoridad Nacional para la Innovación Gubernamental, del Ministerio de la Presidencia, se aprueba el Decreto Ejecutivo No.709 de 2011, con el que crea el Computer Security Incident Response Team, (CSIRT), con el propósito de prevenir e identificar ataques e incidentes de seguridad a los sistemas informáticos de la infraestructura crítica del país (Godoy, 2020, p. 125).

Como se puede apreciar, el gobierno panameño adoptó medidas de seguridad muy fuertes, como la creación de una unidad especial que se dedica exclusivamente a la atención de este delito que crece conforme pasa el tiempo, lo cual es un claro ejemplo de cómo se debe abordar este tema que tanto preocupa a la población.

Si se analiza la situación de esta problemática en los países de la región, como el ejemplo que se presentó con Colombia y Panamá, y se compara la problemática con Costa Rica, se puede apreciar que el modelo de seguridad jurídica de Costa Rica es más simplista, debido a que solamente aborda el problema desde plano legal, específicamente con el tipo penal y no se han adoptado hasta el momento medidas más eficientes para solucionar este mal que afecta al país en general, porque también cabe mencionar que ha habido empresas afectadas con este delito.

Costa Rica no posee una estructura de persecución eficiente como la de Panamá y de prevención como en el caso de Colombia. Es necesario que se realicen cambios en el sistema judicial y en la política de persecución criminal en estos casos, para abordar este problema de una forma más rápida y efectiva, a lo mejor mediante la adopción de algunas de las soluciones planteadas por otros países de la región.

Por otra parte, con respecto a la estructura del delito del fraude electrónico, se puede identificar que este se consuma desde el momento en que la entidad financiera aprueba la transferencia y una vez hecha es muy difícil revertirla, porque el dinero fue transferido electrónicamente a otra cuenta. Entonces se estaría ante una situación muy particular, que sería la posible atribución de cierto grado de responsabilidad a los bancos por el hecho de haber aprobado ciertas transferencias sin las medidas de seguridad mínimas. Se estaría ante el supuesto de “la responsabilidad bancaria frente a los fraudes electrónicos” (Rodríguez, 2014, p. 289).

Por consiguiente, se puede señalar que,

> se debe partir del supuesto de que por tratarse de responsabilidad subjetiva, la entidad bancaria está obligada a desarrollar sus actividades tendientes a brindar seguridad en transacciones electrónicas con el mayor grado de diligencia, pero no puede garantizar un resultado, pues trascendería entonces su obligación al ámbito de la responsabilidad objetiva (Rodríguez, 2014, p. 293).

Como se logró observar, los bancos son responsables de los mecanismos de seguridad, que en la medida de lo posible son impenetrables con la debida diligencia de sus clientes. En cuanto al resultado, se debe resaltar que el cliente también tiene su

grado de responsabilidad cuando manipula estos sistemas, en relación con la debida diligencia en la administración de la información confidencial como, por ejemplo, guardar en un lugar seguro las claves de acceso con la total certeza de que nadie más tendrá acceso a esos datos.

Ahora bien, en el caso del banco, al realizar una actividad económica con alto grado de diligencia, debe tomar en consideración la teoría del riesgo que según Rodríguez (2014), "que tiene tres vertientes principales: "En primer lugar, en el escenario del riesgo creado, quien en desarrollo de una actividad genere un riesgo, está en la obligación de indemnizar los perjuicios que de este devengan sobre terceros" (p. 295). En este supuesto, se logra inferir que esta teoría viene a atribuir la responsabilidad a quien generó el riesgo del fraude, en consecuencia se debe indemnizar si la otra parte obra de buena fe y de una forma responsable al tomar en cuenta todas las medidas de seguridad necesarias para realizar la operación financiera. El cliente, aun habiendo tomado todas las medidas de seguridad, siempre sufre el fraude, porque el simple hecho de realizar una operación financiera de forma electrónica ya genera un riesgo que la entidad financiera debe asumir, porque esta misma fue la que puso al servicio del cliente la realización de esta operación financiera por medio de sistemas electrónicos.

> En segundo lugar, bajo la teoría del riesgo provecho, quien ejerza una actividad que genere un riesgo y obtenga de esta una utilidad, un provecho, deberá indemnizar los perjuicios que se causen y que sean derivados de tal riesgo, sin importar si obró o no en forma diligente (Rodríguez, 2014, p. 296).

Esta teoría, como se puede apreciar, menciona que si las entidades financieras obtienen un provecho (económico en este caso), deberán obrar de buena fe en beneficio de la protección de los datos confidenciales de sus clientes, debido a que al tratarse de actividades financieras que generan utilidades de gran importancia para la propia existencia de la entidad, esta debe indemnizar en caso de algún perjuicio en el supuesto de alguna negligencia por parte del cliente, es decir, la entidad debe ayudar a su cliente informándole y brindándole las herramientas de seguridad necesarias para prevenir el hecho delictivo, y si el cliente de buena fe obra de forma errónea, debe obtener una indemnización por el daño sufrido.

Finalmente, en tercer lugar está el riesgo profesional, que consiste en "el riesgo derivado de las actividades que requieren un cierto grado de profesionalismo, como podría ocurrir con las profesiones liberales, en especial la responsabilidad médica, y otras como la actividad financiera" (Rodríguez, 2014, p. 296). En este caso se puede inferir que no es posible atribuir la responsabilidad de este riesgo a una persona que no

tiene conocimiento de lo que significan los peligros de realizar operaciones financieras sin las medidas de seguridad necesarias para evitar la exposición ante el posible fraude electrónico, además de su inexperiencia con el tema, a diferencia de la entidad financiera, que está sumamente relacionada con esta actividad económica, lo cual demuestra su experiencia día a día con dichos eventos.

Ahora bien, por otra parte, están los casos en los que la responsabilidad recae en la víctima, debido a que "corresponde más precisamente a un conjunto heterogéneo de supuestos de 'hecho', en los que se incluyen no sólo comportamientos culposos en sentido estricto, sino también actuaciones anómalas o irregulares del perjudicado que interfieren causalmente en la producción del daño" (Paz, 2018, p. 270). En estos casos se logra deducir que el daño sufrido lo provoca la misma víctima, se le atribuye la responsabilidad por su posible actuar negligente causando el daño económico.

No obstante, aunque la responsabilidad de la puesta en peligro recaiga en la víctima en la mayoría de los casos, las entidades financieras deben tomar medidas de prevención debido a que "uno de los principales riesgos a los que están sometidas las entidades financieras son los ataques de fraudes electrónicos. Billones de dólares en pérdidas son absorbidas cada año por las entidades financieras debido a transacciones fraudulentas" (Álvarez, 2020, p. 81). Por esta razón es de suma importancia que las entidades financieras tomen las medidas necesarias para disminuir la incidencia de estos delitos. Se debe considerar que no es solo por el perjuicio económico que esto produce, también se debe tener presente el tema del prestigio financiero que la entidad bancaria debe proteger para lograr atraer más clientes, porque para nadie es un secreto que si un banco o entidad financiera saliera en los titulares de noticias como la entidad donde sus clientes sufren mayor cantidad de fraudes, esto generaría un cierto grado de desconfianza por parte de las personas para guardar su dinero y realizar operaciones financieras.

Es por esta razón que las entidades financieras deben tomar medidas avanzadas tales como la implementación de sistemas de prevención, por ejemplo,

> la minería de datos y el aprendizaje automático son métodos populares para estudiar y combatir los casos de fraude con tarjetas de crédito. Existe una gran cantidad de estudios que explotaron la fuerza de la minería de datos y el aprendizaje automático para prevenir las actividades fraudulentas con tarjetas de crédito (Álvarez, 2020, p. 85).

Este es un claro ejemplo de la tecnología llamada "machine learning en la detección de fraudes de comercio electrónico aplicado a los servicios bancarios"

(Álvarez, 2020, p. 81). Por esta razón, esta tecnología es tan ingeniosa que, al momento de detectar una transacción sospechosamente fraudulenta, inhabilita automáticamente los sistemas de transferencias electrónicas, incluidas las tarjetas asociadas a la cuenta bancaria.

Es un sistema muy necesario y casi imprescindible en cualquier entidad financiera, porque al bloquear la tarjeta ante una transferencia sospechosa, se evita un perjuicio económico mayor dependiendo de la situación, que el banco debe asumir si la responsabilidad de la puesta en peligro no recae en la víctima.

Conclusiones

Como se logró observar anteriormente, este delito es un tema complejo en el cual el perpetrador tiene un abanico de posibilidades para llevar a cabo su objetivo final, el cual consiste en el perjuicio económico de la víctima. En el caso de Costa Rica, "las pérdidas asociadas a esta modalidad delictiva ya ascienden a alrededor de $1 millón por lo que se hace apremiante prevenir a la ciudadanía para que eviten ser víctimas de este delito y la pérdida de su dinero" (Hidalgo, 2021, párr. 17). Por esta razón las autoridades deben tomar las medidas necesarias para resolver estos casos tan complejos y avanzados tecnológicamente hablando.

En el mundo globalizado actual es muy común escuchar que un *hacker*, desde otro país, a miles de kilómetros de distancia, puede realizar un fraude electrónico con solamente una llamada telefónica o un correo electrónico infectado con un virus informático, es por esto que países como los Estados Unidos invierten muchísimo de su presupuesto en ciberseguridad, un ejemplo es la Unidad contra Delitos Cibernéticos del Departamento de Seguridad Nacional; esta unidad "contra delitos Cibernéticos del C3 provee la gestión y supervisión de investigaciones para la agencia relativas al internet al focalizarse en las organizaciones criminales transnacionales que utilizan funciones o elementos cibernéticos para extender sus actividades criminales" (Centro Contra Delitos Informáticos de los Estados Unidos de América ICE, 2022, párr. 4).

Este centro se especializa exclusivamente en delitos cibernéticos, entre los cuales están los delitos económicos cibernéticos. Costa Rica necesita una unidad que atienda estos delitos, porque si bien es cierto que se posee una legislación que castiga estos hechos criminales, no se cuenta con una unidad que tenga las herramientas idóneas para investigar estos delitos. Estados Unidos, además de otros países de la región como Colombia y Panamá, en este caso serían un ejemplo para seguir en cuanto a la lucha contra el delito del fraude electrónico se refiere.

Referencias

Acurio, S. (s. f.). *Delitos Informáticos: Generalidades.* https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Álvarez, F. (2020). Machine Learning en la detección de fraudes de comercio electrónico aplicado a los servicios bancarios. *Revista de Ciencia y Tecnología*, 20, 81–95. https://dialnet.unirioja.es/servlet/articulo?codigo=7763844

Asamblea Legislativa de la República de Costa Rica. (1970). *Ley N.º 4573. Código Penal.* http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=96389&strTipM=TC

Banco Central de Costa Rica. (2022). *SINPE Móvil.* https://www.bccr.fi.cr/sistema-de-pagos/servicios-brindados-a-clientes/sinpe-m%C3%B3vil#:~:text=SINPE%20M%C3%B3vil%20se%20dirige%20al,Web%20M%C3%B3vil%2C%20Banca%20App%2C%20Banca

Castro, J. (2021, 22 de marzo). Denuncias por fraudes informáticos se dispararon en 2020. *La República.* https://www.larepublica.net/noticia/denuncias-por-fraudes-informaticos-aumentaron-en-un-60

Díaz, N. (2022, 4 de mayo) 1.790 clientes del Banco Nacional fueron víctimas de fraude informático por ₡1.619 millones y $495 mil. *Semanario Universidad.* https://semanariouniversidad.com/pais/1-790-clientes-del-banco-nacional-fueron-victimas-de-fraude-informatico-por-%E2%82%A11-619-millones-y-495-mil/

Dictionary.com. (2022). https://www.lexico.com/es/definicion/electronica

Gabaldón, L. (2006, mayo-agosto). Fraude electrónico y cultura corporativa. *Cuaderno CRH*, *19*(47), 195-213. https://www.redalyc.org/pdf/3476/347632169004.pdf

García, R. (s. f.) *Seguridad informática y el malware*. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2641/00004128.pdf?sequence=1

Godoy, J. (2020). Regulaciones panameñas a los delitos informáticos que afectan los Sistemas de Información Contables Administrativos (SICA). *Revista Científica Orbis Cógnita*, *4*(1), 113–134. **h**ttps://doi.org/10.48204/j.orbis.v4n1a8

Hernández, A. (s. f.). *Evolución de las computadoras.* https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/20050/evolucion-computadoras.pdf?sequence=1&isAllowed=y

Hidalgo, A. (2021, 23 de marzo). EF Explica: Estas son los timos más comunes de los estafadores para robar el dinero de las cuentas de las personas. *El Financiero.* https://www.elfinancierocr.com/finanzas/ef-explica-estas-son-los-timos-mas-comunes-de-los/Q4CCRQVCNZFQXCALWCCH446SGQ/story/

Marín A. (2022). *Un tercio de los hogares del país ha sufrido estafa o intento de estafa.* https://www.ucr.ac.cr/noticias/2022/02/01/un-tercio-de-los-hogares-del-pais-ha-sufrido-estafa-o-intento-de-estafa-por-medios-digitales-desde-que-inicio-la-pandemia.html

Moreno, J., Sánchez, C., Salavarrieta, J. y Vargas, L. (2019). Soluciones tecnológicas para la prevención de fraude y diseño de un modelo de prevención del riesgo transaccional para el botón de pago. *Entre Ciencia e Ingeniería.* (26), 36-42. https://doi.org/10.31908/19098367.1154.

Oficina de Investigaciones de Seguridad Nacional. (2022). *Centro Contra Delitos Cibernéticos. ICE, USA.* https://www.ice.gov/es/investigaciones/delitos-ciberneticos

Oxman, N. (2013, segundo semestre). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". *Revista de Derecho*. (XLI). 211 – 262. https://vlex.cl/vid/estafas-informaticas-traves-internet-648790365

Paz, A. (2018). La culpa del consumidor en la responsabilidad financiera y su proyección causal en el daño por fraude electrónico. Una mirada a la jurisprudencia de la delegatura para funciones jurisdiccionales de la superintendencia financiera de Colombia. *Revista de Derecho Privado,* 35, 261 – 289.

Real Academia Española. (2022). *Diccionario de la lengua española*. (23.ª ed.), https://dle.rae.es

Rodríguez, A. (2014). Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos: el riesgo provecho, el riesgo creado y el riesgo profesional. *Vniversitas*, 128, 285–314. https://doi.org/10.11144/Javeriana.VJ128.aerb

Sain, G. (s. f.) Evolución histórica de los delitos informáticos. *Revista Pensamiento penal.* https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.pdf

Sandoval, J. (2011). Ingeniería social: corrompiendo la mente humana. *Revista Seguridad*, 10. https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

Santillán, J. y Becerril, S. (2009). Fraude electrónico. *Revista Seguridad*, 2. https://revista.seguridad.unam.mx/numero-02/fraude-electr%C3%B3nico

SEFAIR, A. P. (2018). La culpa del consumidor en la responsabilidad financiera y su proyección causal en el daño por fraude electrónico. Una mirada a la jurisprudencia de la Delegatura para Funciones Jurisdiccionales de la Superintendencia Financiera de Colombia. *Revista de Derecho Privado*, 35, 261–289. https://doi.org/10.18601/01234366.n35.10

Silva, C. (2016, 14 de junio). Geolocalización de teléfonos celulares. *Ingeniería de las telecomunicaciones.* https://blog.telecom.pucp.edu.pe/index.php/2016/06/14/geolocalizacion-de-telefonos-celulares/