“Phishing y la responsabilidad de entidades bancarias con los usuarios del sistema bancario”

Romeo Lucas Bernal Borja
(El Salvador)

Maestría en
Derecho Privado

PHISHING Y LA RESPONSABILIDAD DE ENTIDADES BANCARIAS CON LOS USUARIOS DEL SISTEMA BANCARIO

Romeo Lucas Bernal Borja

RESUMEN

En el presente artículo se analiza la responsabilidad bancaria frente a los fraudes electrónicos cometidos en contra del sistema financiero y sus usuarios, haciendo un acercamiento al ámbito del derecho privado en cuanto a la dinámica de los contratos bancarios, el uso de las aplicaciones informáticas para la dinámica comercial y los niveles de seguridad de estas. Luego de esto, se ahondará en el ámbito penal en cuanto al tema de los delitos informáticos; de esta forma se analizará el tema de phishing, sus características, modalidades y fines delictivos que persigue, para realizar el enfoque en lo referente a los delitos de hurto y estafas informáticas; asimismo, se abordará el tema del régimen de la responsabilidad subjetiva y objetiva de las instituciones financieras, en los supuestos cuando los usuarios del sistema financiero son víctimas de fraudes y se les ha sido sustraído el dinero de los contratos de depósitos o de apertura de créditos rotativos, a través de engaños o hurtos de identidades suplantando tanto a la institución financiera como a los usuarios. Concluyendo en una responsabilidad compartida para satisfacer los daños, en los supuestos de debida diligencia, responsabilidad de resguardo y custodia para el banco, en contraposición a la debida diligencia en el uso de sus datos por parte de los usuarios de los sistemas bancarios.

PALABRAS CLAVE: phishing - patrimonio - big data - datos personales - banca móvil - responsabilidad bancaria - delito informático - hurto informático - estafa informática.

PHISHING AND THE RESPONSIBILITY OF BANKING ENTITIES WITH THE USERS OF THE BANKING SYSTEM

Romeo Lucas Bernal Borja

ABSTRACT

In this article it will be analyzed the bank's responsibility in the face of electronic fraud committed against the financial system and its users, making an approach to the field of private law in terms of the dynamics of banking contracts, the use of computer applications for commercial dynamics and its security levels. After that, it will be addressed the criminal field regarding the subject of computer crimes, thus it will be analyzed the topic of phishing, its characteristics, modalities and the criminal purposes it pursues, and subsequently focus on the crimes of computer theft and fraud. Likewise, it will be addressed the subject of subjective and objective responsibility regime of financial institutions banks, in the cases when financial system's users are victims of fraud and their money has been stolen from the deposit or revolving credit opening contracts, through deception or identity theft impersonating both the financial institution and the users. Concluding in a shared responsibility to satisfy the damage in cases of due diligence, safeguard responsibility and custody for the bank, as opposed to the due diligence in the use of their data by the users of the banking systems.

KEYWORDS: phishing - wealth - big data - personal data - mobile banking - banking responsibility - computer crime - computer theft - computer fraud.

Phishing y la responsabilidad de entidades bancarias con los usuarios del sistema bancario

Romeo Lucas Bernal Borja[1]
(El Salvador)

Introducción

El presente artículo bibliográfico aborda el impacto que tiene el *phishing* en la sociedad y los inconvenientes que está generando a nivel nacional; actualmente, con el avance desmesurado de la era digital, gran parte de las personas asalariadas y empresarios, hacen uso de aplicaciones electrónicas para manejar su dinero, aplicaciones proporcionadas por las instituciones bancarias y conocidas como "Banca Móvil", que logran dinamizar las operaciones bancarias, descongestionan las agencias bancarias, y acercan los productos financieros a los clientes; las mismas se han vuelto un peligro real, ya que en la mayoría de ocasiones carecen de seguridad contra hackeos, clonaciones y/o suplantación de las identidades, situaciones que ponen en riesgo el patrimonio de los usuarios y del sistema bancario.

1 Licenciado en Ciencias Jurídicas, egresado de la Maestría de Derecho Privado de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad de El Salvador, docente académico y agente fiscal de la Fiscalía General de la Republica de El Salvador.

Al analizar las consecuencias del *phishing* como una situación que ataca directamente el patrimonio de los clientes y del banco, se debe de encuadrar en un ejercicio de tipicidad de delitos informáticos, este articulo no persigue específicamente esa circunstancia, sino analizar los eventos que surgen cuando ya se ha configurado el delito como tal; su resultado, es el despojo del patrimonio de la víctima; y en consecuencia el análisis sobre quién que debe solventar la situación, como la sustracción no autorizada del dinero en las cuentas del cliente.

Asimismo, es de hacer notar que durante la pandemia del COVID-19 estas acciones han tenido un impacto significativo en la criminalidad, donde una gran cantidad de clientes de los bancos se han visto en la necesidad de solicitar la tutela de sus derechos patrimoniales a través de Fiscalía General de la Republica, Defensoría del Consumidor, Superintendencia del Sistema Financiero y la red de bancos del país, donde es menester verificar las formas que tienen estas y otras instituciones para regular tal circunstancia, y a la vez tutelar tales los derechos de los clientes en sus relaciones de consumo y en sus relaciones de contratos bancarios; además, es necesario determinar el grado de responsabilidad de las instituciones bancarias y demás participantes.

Debido a lo anterior, el *phishing* ha cobrado relevancia al punto que es necesario el análisis de las leyes, como derecho aplicable en el país, criterios jurisprudenciales y demás modelos doctrinarios que desarrollan los requisitos, características, formas de prevención, sobre todo la determinación de las obligaciones derivadas de los contratos y del derecho de consumo frente a las entidades bancarias; buscando además comprender la evolución del phishing, sus componentes como el engaño, el cual es de relevancia penal, así como la determinación de cuales casos se encuentran frente a una responsabilidad bancaria y en qué casos el cliente o usuario no tendrá protección o respuesta por el sistema financiero.

Breve introducción a la digitalización y modernización de la banca

En la actualidad el *internet banking* se cuenta dentro de los servicios que componen la categoría de "banca electrónica". Este término supone una modificación al esquema tradicional de comunicación entre el banco y sus clientes, realizado en forma presencial y documentado en soportes de papel con firmas autógrafas. El avance vertiginoso en materia de telecomunicaciones e informática ha generado para los bancos al igual que para muchos otros sectores económicos, nuevas posibilidades de prestación de servicios, con una reducción importante en materia de costos y alcanzando fronteras de mercado mucho más amplias, ventajas tangibles tanto para el prestador como para el usuario de los servicios.

A pesar de que se tiende a equiparar el concepto de *internet banking* con el de banca electrónica, lo cierto es que esta última es una construcción más amplia, de la cual la banca en línea es solo una faceta. El *internet banking* comprende una serie de herramientas que una entidad bancaria pone al alcance de los clientes, con el objeto de que puedan realizar sus operaciones bancarias y financieras, a través de un ordenador y mediante la conexión a internet. La función principal de la banca por internet es la de permitir al usuario el acceso y administración de los fondos de sus cuentas, sean estas de ahorro, corrientes o electrónicas, por medio de la red global.[2]

Para acceder a los servicios de banca por internet, es necesario que el cliente tenga una cuenta en estado activo, ya sea corriente, electrónica o de ahorros, el plástico (tarjeta de débito o crédito) asociado a la cuenta y la información de uso privilegiado que le fue entregada por parte del banco para la operación de estas. En sentido inverso, para operar cuentas corrientes o de ahorros no es necesaria la suscripción del servicio de *internet banking*, este

2 Genaro Jiménez Orozco, "Distribución del Riesgo y Análisis de Responsabilidad en los casos de Fraude Informático bajo la modalidad de Phishing. Aplicación de la Ley de Protección y Defensa Efectiva del Consumidor". (Tesis de Licenciatura. Facultad de Derecho de la Universidad de Costa Rica, 2012), 111.

último es un plus que se le ofrece a los clientes y no una imposición asociada al manejo de las cuentas. No sería legítimo por parte de un banco condicionar la prestación de un servicio a la suscripción de otro, que en tesis de principio no le es indispensable.[3]

Al momento de realizar el registro en línea, los sistemas de los diferentes bancos van a solicitar al cliente la verificación de una serie de información que se encuentra estandarizada y algunos otros datos que responden a medidas o dispositivos de seguridad diversos. Con la proliferación de los fraudes y dado que la tecnología fue permitiendo avances en la materia, se implementaron nuevas modalidades de verificación; este proceso es lo que se conoce como autenticación, que está íntimamente vinculada al tema de seguridad informática.[4]

La autenticación,[5] para el tema que nos ocupa, se va a entender como la forma en que un sistema verifica o se asegura que un usuario que intenta acceder y realizar acciones dentro del sistema, es quien dice ser y tiene autorización para hacer lo que pretende. En otras palabras, el sistema no pretende entonces identificar a una persona, sino autenticar que sea quien dice ser. Los sistemas de autenticación de usuarios se dividen por lo general en tres categorías:

3 Gustavo Sain, *Cibercrimen y delitos informáticos, los nuevos tipos penales en la era de internet.* (1ra Ed, Ciudad Autónoma de Buenos Aires: Erreius, 2018), 18. La seguridad informática es entendida como cualquier acción que impida la ejecución de operaciones no autorizadas sobre un sistema informático o red de computadoras. En líneas generales, comprende el conjunto de medidas preventivas, de detección y corrección destinadas a proteger los recursos informáticos de una organización.

4 Martha Irene Romero Castro et al, *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades.* (Universidad Estatal del Sur de Manabi, Ecuador, 1era Ed, 2018), 13. La seguridad informática se encarga de la seguridad del medio informático, la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático.

5 Gustavo Sain, *Cibercrimen y delitos informáticos, los nuevos tipos penales en la era de internet.* (1ra Ed, Ciudad Autónoma de Buenos Aires: Erreius, 2018), 19. Sobre este punto lo contrato a la autenticación es la vulnerabilidad informática es una debilidad que presenta un sistema informático que puede permitir que las amenazas causen daños en los mismos. Un incidente de seguridad, por su parte, puede ser definido como un evento que puede producir una interrupción de los servicios brindados por un sistema informático, causando así pérdidas materiales o financieras a la organización

1. Algo que el usuario sabe, como una contraseña.
2. Algo que el usuario tiene, como una tarjeta de identidad, *smart card* o dispositivos OTP.
3. Algo que el usuario es: una característica física del usuario o sistemas basados en un acto involuntario del usuario; esto es autenticación biométrica.

Un sistema de autenticación eficiente debería combinar al menos dos de las anteriores categorías para elevar el nivel de seguridad y disminuir el riesgo; todo sistema de autenticación debe adicionalmente responder a parámetros de viabilidad.

El primero de dichos parámetros debe necesariamente ser el de seguridad, esta debe ser muy elevada con márgenes de error lo más cercanos a cero posible, capaz de soportar las amenazas o ataques. El segundo parámetro es el de costos; evidente que tratándose de seguridad se debe hacer una relación entre el valor de lo que se necesita proteger y el costo de los mecanismos de seguridad. Un sistema en el que el costo de seguridad es más alto que lo que se quiere proteger, está fuera de balance y no es rentable.

En este sentido, la autentificación del titular de la cuenta esta verificado por el mismo sistema de bancos, que en mayor o menor medida es quien pone a disposición los niveles se seguridad de la banca en línea, no importando el segundo parámetro, ya que su masificación en la prestación de los servicios bancarios le permite a cada entidad asumir el costo de la obtención y mantenimiento del sistema. Dada esta particularidad, el nivel de seguridad frente a los ataques de *phishing* depende en gran medida de los niveles de autentificación del banco.[6]

6 Genaro Jiménez Orozco, "Distribución del Riesgo y Análisis de Responsabilidad en los casos de Fraude Informático bajo la modalidad de Phishing. Aplicación de la Ley de Protección y Defensa Efectiva del Consumidor" (Tesis de Licenciatura. Facultad de Derecho de la Universidad de Costa Rica, 2012),112.

Definiciones de phishing

El *phishing* es una derivación directa de origen inglesa, de la palabra *fishing,* cuya traducción significa "acción de pescar"; en su aplicación práctica para fines informáticos se agregan las letras "PH", que deviene de las palabras "*password harvesting*", en consecuencia la traducción implica la "acción de pescar datos". A partir de ello, el término toma relevancia en el ámbito jurídico, ya que conlleva una intención defraudadora, que ataca el patrimonio del sujeto pasivo con la finalidad de apoderarse de dicho patrimonio, obteniendo un lucro para si o para un tercero, encajando en los casos típicos de estafas.[7]

Por otra parte, también puede definirse como una modalidad de fraude por medio del cual, el delincuente informático o ciberdelincuente engaña al sujeto pasivo mediante un correo electrónico que supuestamente le dirige una entidad bancaria o estatal para que la víctima haga clic en el supuesto enlace, redirigiéndolo así a una página web que ha suplantado a la entidad oficial, dándose el caso que, cuando la persona ingresa a dicho sitio web, coloca su información personal, la cual es obtenida por el ciberdelincuente.[8]

Es por ello que el *phishing* es el mecanismo más efectivo para cometer fraudes informáticos, ya que estos ataques buscan robar datos de identificación personal de los consumidores, así como sus credenciales de cuentas financieras a través de correos electrónicos con enlaces que conducen al sujeto pasivo a sitios webs falsos que han sido diseñados con la única finalidad de estafar a la persona quien comparte sus números de tarjeta, credenciales, nombres de usuario, entre otros; además, generalmente el cibercriminal generalmente se vale del uso de artilugios técnicos como la instalación de *crimewear* a través de troyanos que captan las pulsaciones del teclado.

En otras palabras, el *phishing* consiste en robar información del usuario sin que este se percate de lo sucedido. Todo esto en razón de que el ciberdelincuente se basa en la ingeniería social, que es la forma de aplicar

7 *Ibid.* 145.

8 Jaime Rincón Arteaga et al, "Impacto económico y social del phishing y el smishing en Colombia y el mundo", *Revista Banca y Economía, Revista N° 1259*, (2020): 4.

determinados conocimientos psicológicos y sociológicos fundamentales. Es decir, no se trata de conocimientos excesivamente complejos porque el atacante normalmente no dispone de muchos detalles de su víctima y tiene que basarse en generalidades estadísticamente válidas para obtener, en la misma proporción, resultados estadísticamente positivos. La ingeniería social se nutre inicialmente de una serie de conceptos básicos y estadísticamente ciertos de la psicología del individuo.[9]

Sin embargo, es evidente que el *phishing* va más allá del engaño, ya que su naturaleza es la obtención de la información confidencial y personal de manera ilegitima a través del engaño,[10] sin que el fin inmediato sea un provecho en específico, el cual solo adquiere relevancia cuando involucra a la responsabilidad bancaria a efecto de lograr la restitución del dinero perdido. En ese sentido, el *phishing* es un mecanismo criminal que consiste en el uso de técnicas de engaño y códigos maliciosos con la finalidad de obtener información confidencial o personal relacionada a una persona especifica.[11]

9 Martha Irene Romero Castro et al, *Introducción a La Seguridad Informática y El Análisis de Vulnerabilidades.* (Universidad Estatal del Sur de Manabi, Ecuador, 1era Ed, 2018), 46. La ingeniería social es el principal método de distribución de ransomware, un malware que cifra los archivos y pide un rescate económico. El Phishing funciona porque el email parece auténtico, suplanta la identidad corporativa de una empresa reconocible, el caso del espía Phishing es una variación del Phishing que, en lugar de distribuirse masivamente, emplea email redactados y diseñados para engañar específicamente a una persona. Es común suplantar a un miembro de la compañía de posición jerárquica, a un proveedor o aun cliente, así consiguen crear una historia consistente capaz de engañar a la víctima específica mediante la ingeniería social.

10 *Vid*. Christopher Hadnagy, *Ingeniería Social: El arte del hacking personal.* (Ediciones Anayamultimedia, España, 2011), 78.

11 Alejandro Rodríguez Zárate. "Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos: el riesgo provecho, el riesgo creado y el riesgo profesional", *Revista Universitas. N° 128*. (2014): 23.

Características

La característica principal del *phishing*[12] es el engaño con el que se somete al usuario o titular de la información haciéndole creer que está entregando la información a una entidad oficial y confiable. Pero que, al final, acaban hurtando su información y realizando actividades; suplantando su identidad sin que este preste su consentimiento y, en muchas ocasiones, ni siquiera se percata en el momento, induciéndolo al error para que un tercero, de mala fe, utilice su información con diversas finalidades, pero que la principal es la obtención de un provecho injusto a costa del patrimonio del sujeto pasivo.

Otra de las características del *phishing* es su objetivo, el cual consiste en la obtención de datos del titular con la finalidad de utilizar su información en negocios jurídicos como que si la victima fuera quien los ha realizado, comprometiendo la seguridad de los bancos y poniendo en riesgo el comercio electrónico, ya que lleva a la pérdida de confianza hacia el sistema bancario, lo cual es esencial para que el mercado funcione.[13]

Generalmente, el delincuente es difícil de ubicar geográficamente debido a la ventaja tecnológica que estos tienen, ya que remotamente pueden obtener la información personal y bancaria, no importando si esta persona está dentro o fuera del país, lo que les permite escabullirse de las sanciones legales penales correspondientes y, en consecuencia, dificulta el uso de soluciones jurídicas

12 Jaime Rincón Arteaga et al, "Impacto económico y social del phishing y el smishing en Colombia y el mundo", *Revista Banca y Economía, Revista N° 1259,* (2020): 4. El phishing y el smishing son dos modalidades de fraude por medio de las cuales los ciberdelincuentes engañan a las personas mediante un correo electrónico (phishing) o un mensaje de texto (smishing), que supuestamente llega de parte de una entidad oficial, como una entidad bancaria o la DIAN, entre otras, para que el usuario haga clic en el enlace que viene en el cuerpo del correo o mensaje. Cuando el usuario hace clic en el enlace es redirigido a una página web que suplanta la página original de la entidad, por lo tanto, cuando la persona ingresa cualquier información en esta como usuarios y contraseñas, la información viaja directamente al ciberdelincuente.

13 Nicolás Oxman, "Estafas informáticas a través de Internet", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, N° 41.* (2013): 215. La finalidad común es la de 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 "mula".

para hacer frente a esta problemática. Asimismo, como se verá más adelante, el *phishing* conlleva un grado de culpa para la víctima ya que entrega su información cuando es engañado y podría alegarse que es quien se coloca en riesgo.[14]

Tipos y modalidades del phishing

Como se mencionaba anteriormente, el *phishing*[15] es un mecanismo para cometer fraudes informáticos en el cual el delincuente, a través del uso de la información del titular, realiza transferencias electrónicas, efectúa retiros o realiza compras sin el consentimiento del mismo; en ese sentido, de manera doctrinaria se identifican dos modalidades de *phishing*.[16]

a. *Phishing* por engaño: se desarrolla con el uso desmesurado de las redes sociales, donde se mantiene la naturaleza con el mismo fraude que siempre ha existido, pero desde los medios electrónicos los cuales han sido puestos a disposición de la sociedad quienes, en su mayoría, carecen de un nivel de preparación para poder identificarlo. Esta modalidad se configura cuando el ciberdelincuente entra en contacto con el usuario generalmente por medio de mensajes de texto o correos electrónicos, haciéndose pasar por una entidad financiera, comercial o gubernamental oficial, para generarle confianza al usuario a efecto de conseguir que el usuario le brinde datos confidenciales.[17]

14 Marcos Rodríguez Puentes, "Responsabilidad bancaria frente al phishing" (Tesis de Maestría, Facultad de Derecho, Ciencias Políticas y Sociales Departamento de Derecho Bogotá, Colombia. 2015), 20.

15 Nicolás Oxman, "Estafas informáticas a través de Internet", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso,* N° 41. (2013): 217.

16 Marcos Rodríguez Puentes, "Responsabilidad bancaria frente al phishing" (Tesis de Maestría, Facultad de Derecho, Ciencias Políticas y Sociales Departamento de Derecho Bogotá, Colombia. 2015), 30.

17 Nicolás Oxman, "Estafas informáticas a través de Internet", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, N° 41.* (2013): 215. En efecto, mientras en el "phishing" no se utiliza otra cosa que el correo electrónico como soporte material para reconducir a la víctima a un sitio "web" falso12, en el "pharming" lo que se introduce es un malware o un gusano en el servidor de Internet del usuario para reconducirlo mediante la manipulación del "Domain Name Server" (DNS) a una página "web" falsa.

b. *Phishing* basado en software malicioso: consiste en la instalación de un virus en el dispositivo del usuario, a efecto de vulnerar el sistema de seguridad del mismo. Generalmente se logra cuando el ciberdelincuente consigue que el usuario instale el virus por medio de un archivo adjunto, el acceso a un enlace o al haber descargado un programa o aplicación.[18] En estos casos, el ciberdelincuente utiliza al usuario y al servidor web para poder atrapar la información con distintas finalidades sin que el usuario se percate de lo que está sucediendo, pudiendo derivar en el robo de la información, para posteriormente venderla o apoderarse de las cuentas del usuario con la finalidad de drenar su patrimonio.[19] Sobre este punto, es importante atender que esta forma de *phishing*, recibe el nombre de "*pharming*".[20]

Phishing en el ámbito penal como delito informático

El delito informático hace referencia a las actividades delictivas o conductas típicas en las que el componente informático se hace indispensable para su perpetración, o sea que el medio informático no puede suprimirse o, de otra forma, la acción delictiva no sería posible. Es decir, es la acción delictiva que realiza una persona con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, ya sea a través de hardware o software. En términos generales, se habla de conductas típicas y sancionables

18 Eduardo Benavides, Walter Fuertes, Sandra Sánchez, "Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura", *Revista Ciencia y Tecnología, N° 13* (2020): 13.

19 Marcos Rodríguez Puentes, "Responsabilidad bancaria frente al phishing" (Tesis de Maestría, Facultad de Derecho, Ciencias Políticas y Sociales Departamento de Derecho Bogotá, Colombia. 2015), 131.

20 Michel Paulina Martínez Padilla, "*La responsabilidad bancaria frente a los delitos informáticos*". (Tesis de Maestría, Universidad Andina Simón Bolívar. Ecuador, 2015), 33. En el pharming el sujeto activo del delito clona una página institucional como, por ejemplo, de una entidad bancaria o de una compañía de comercio electrónico, y el usuario de ésta ingresa sus datos para realizar una transacción sin conocer que es falsa.

penalmente, que tienen como eje central el uso antijurídico de un medio informático. Quedan excluidos de esta conceptualización aquellos delitos en los que, pese a que se utilice algún medio o elemento informático, este no sea esencial en el desarrollo de la acción.

Tratándose de delitos informáticos, los intervinientes son el perpetrador de la conducta antisocial, al que se denominará sujeto activo, y el ente sobre el cual recae la conducta del sujeto activo, el cual se puede llamar sujeto pasivo.

Tanto el sujeto activo como el pasivo pueden estar representados por una o varias personas o entes. El sujeto activo, según la doctrina mayoritaria, no es un criminal común, sino que posee conocimientos técnicos especializados que le permiten cometer los ilícitos. El hecho de que posean estos conocimientos hace presumir que se trata de personas ubicadas en una cierta esfera socioeconómica. Esta afirmación no puede ser tomada como irrefutable, esto en la medida en que muchas personas que se dedican al crimen informático son autodidactas y que el acceso a un computador es mucho más factible, sin que necesariamente se tenga que tener un nivel económico alto.

Por otro lado, el sujeto pasivo puede estar representado por un sin número de entes, desde personas naturales hasta empresas nacionales o extranjeras, gobiernos y, en general, cualquier organización que se sirva de sistemas automatizados de información para el cometimiento del delito encaminado a obtener un provecho patrimonial.[21] En relación con el sujeto pasivo, se ha distinguido una problemática importante en el sentido que, comúnmente, el ataque informático revela vulnerabilidades en la administración de los sistemas y por ende de los servicios que preste a la víctima.[22]

21 Jesús Francisco Espinosa Sánchez, "Ciberdelincuencia. Aproximación criminológica de los delitos en la red", *La Razón histórica: revista hispanoamericana de historia de las ideas políticas y sociales. N° 44,* (2019): 159. Los ciberdelitos de carácter económico, son aquellos delitos cuyo fin último es la obtención de una recompensa pecuniaria, a través de diversas herramientas online que varían en función y modo de ejecución. El sector privado y, por ende, las grandes multinacionales, así como las medianas y pequeñas empresas (PYMES), se constituyen como los principales focos de acción de dichas acciones ilícitas, debido, en gran parte, a su poder económico.

22 Marcos Rodríguez Puentes, "Responsabilidad bancaria frente al phishing" (Tesis de Maestría, Facultad de Derecho, Ciencias Políticas y Sociales Departamento de Derecho Bogotá, Colombia. 2015), 137.

En ese sentido, el *phishing* reviste relevancia de índole penal patrimonial por las modalidades de obtención de información y el daño que causa al obtener el patrimonio del sujeto pasivo que soporta los delitos de hurto, estafa o extorsión de sus bienes o datos.

Hurto informático, y estafa informática

El hurto por medios informáticos consiste en la manipulación de un sistema informático, mediante la obtención de las autenticaciones por medio de un software malicioso a fin de vulnerar medidas de seguridad para realizar un hurto de las cuentas bancarias de la víctima o también suplantando la identidad de un usuario ante los sistemas de autenticación y autorización establecidos. Bajo estas premisas, para que se configure el hurto se requiere que el sujeto activo obtenga los datos del sujeto pasivo por algún medio y, a partir de ello, sustraiga patrimonio sin el consentimiento de este, ya sea del usuario o directamente al banco. Para este tipo penal es de importante relevancia que la suplantación de datos o identidad vaya encaminada a la sustracción directa por medio del *phishing* en su modalidad "*pharming*" que, a diferencia de la estafa informática, tiene una dualidad de engañados[23] para su materialización.

En este sentido, la estafa informática también tiene relevancia penal ya que, a través de las tecnologías de la información; los ciberdelincuentes disfrazan plataformas fraudulentas por portales seguros para que los usuarios brinden su información mientras un programa almacena sus datos; o también envían un archivo para ser instalado y obtener datos personales y financieros (y utilizarlos suplantado identidades frente al banco). Todo esto demuestra las capacidades en constante transformación con las que cuentan los cibercriminales al momento de realizar la obtención de datos a través de los distintos medios con los que cuentan.[24]

23 Jaime Rincón Arteaga et al, "Impacto económico y social del phishing y el smishing en Colombia y el mundo". *Revista Banca y Economía, Revista N° 1259,* (2020): 5.

24 Oswaldo Ernesto Feusier Ayala, *Comentarios Generales sobre la Delincuencia Informática y la Ley Especial contra Delincuencia Informática y Delitos Conexos. Monográfico. Debates sobre el Sistema de Justicia Penal y Penitenciario.* (Consejo Nacional de la Judicatura, El Salvador, 2016), 213.

Por otro lado, es de mencionar que existe un doble engaño: por una parte al sujeto pasivo, cuando este entrega voluntariamente sus datos bancarios y, por otra parte, cuando el sujeto activo, que ya ha obtenido los datos, engaña al sistema bancario para suplantar al titular de la cuenta, con el fin de obtener el patrimonio, y este entrega voluntariamente dicho patrimonio.[25] Como punto importante, es aquí donde se da el error como elemento de la estafa, donde el uso de distintivos bancarios del sujeto activo engaña al sujeto pasivo y, por otra parte, el error en hacerle creer al sistema bancario que a quien le entrega el dinero es el titular.[26]

Relevancia en el ámbito del derecho privado el phishing

En apartados anteriores se hizo referencia a la capacidad de los cibercriminales de hacer pasar plataformas por portales seguros para que los clientes suministren su información, mientras un programa almacena sus datos, demostrando así que estos actores están en constante desarrollo. Es en relación a esto donde el *phishing* cobra importancia dentro del ámbito del derecho privado, ya que entra en juego la titularidad de los bienes fungibles que son dados por los clientes al banco, tomando en cuenta la naturaleza del dinero y la distribución obligacional de la operación de depósito como contrato básico en la dinámica bancaria, así como el desglose de la obligación del banco respecto a la custodia y obligaciones derivadas, y si de esta puede surgir la restitución o la exención de la responsabilidad por parte del banco quien también ha sido engañado.

Es en esta parte donde es necesario analizar si es posible la restitución de bienes fungibles que fueron confiados a la entidad bancaria y si se encuentra dentro de un régimen de responsabilidad o de obligaciones. Asimismo, es

25 Michel Paulina Martínez Padilla. *"La responsabilidad bancaria frente a los delitos informáticos"*. (Tesis de Maestría, Universidad Andina Simón Bolívar. Ecuador. 2015). 19.

26 Víctor Manuel Rodríguez Luna, Consult, *Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos* (Fiscalía General de la República de El Salvador Escuela de Capacitación Fiscal, y Oficina de las Naciones Unidas contra la Droga y el Delito para Centroamérica y el Caribe, Sin Ed. 2018), 40.

importante determinar hasta dónde es válida la aceptación de la restitución de estos bienes, especialmente cuando el usuario ha brindado su información de forma voluntaria y espontánea sin percatarse que el banco había sido suplantado.

Es así como se plantean dos niveles de protección y responsabilidad, siendo los siguientes:

1. El primero consiste en la proporcionalidad de la protección brindada al consumidor, en las vulnerabilidades del sistema,[27] en relación a la protección que se le brinda por medios tradicionales frente a medios electrónicos.
2. El segundo se compone de la necesidad que el proveedor asuma la responsabilidad por haber optado al uso de medios electrónicos aun sabiendo los riesgos que esto implica, partiendo de la confianza que hay en el sistema electrónico el cual debe ser garantizado por medios jurídicos.

Alcance y naturaleza de la obligación de restitución del banco

En este apartado, es necesario determinar que las especies monetarias cumplen dos funciones importantes, la de ser tratados como cuerpos ciertos y una función meramente económica. Al respecto, es indispensable tomar en cuenta que el dinero común puede ser sustraído de acuerdo a la oferta de ese momento, siendo que este, como cuerpo cierto, es un recurso limitado y único; en todo caso, el dinero equivale a bienes fungibles en razón de que sus unidades son intercambiables, lo que implica que pueda comportarse según la oferta y la

27 Martha Irene Romero Castro et al, *Introducción A La Seguridad Informática Y El Análisis De Vulnerabilidades,* (Universidad Estatal del Sur de Manabi, Ecuador, 1era Ed, 2018), 46. Las vulnerabilidades son por lo general fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso. Si se habla de recursos informáticos se suele decir que una vulnerabilidad es un fallo de diseño de un sistema, un sistema no actualizado o un sistema mal Configurado que permite que un agente externo, acceda sin permisos apropiados al recurso o información que dicho sistema gestiona, en función del tipo de recurso al que estemos orientados existen distintas fuentes de información dónde se puede buscar vulnerabilidades aplicables a los sistemas con que se cuenta.

demanda del momento. Además, cabe recordar que, a mayor emisión de dinero, mayor la inflación y menor su precio; en consecuencia, el dinero se somete a un régimen propio de bienes fungibles, lo que conlleva a la destrucción del vínculo jurídico que une al propietario con la cosa una vez hace uso de este, ya que no es propietario del mismo por habérselo entregado a alguien más.

La posesión del dinero como bien fungible se configura cuando se ejerce la tenencia con ánimo de señor y dueño y se actúa como propietario del bien que se tiene, siempre que se cuente con el poder adquisitivo y dispositivo sobre el mismo. Además, cabe recordar que la propiedad implica, ante todo, la capacidad de enajenar sin perjuicio de que el adquirente este obligado de respetar los gravámenes que recaen sobre el bien.[28]

Ahora bien, el traslado de los bienes fungibles, para interés del tema del *phishing,* responde a que, con el traslado del dinero al banco, por medio de depósitos de ahorro o en cuenta corriente, el titular traslada la propiedad del dinero a la entidad bancaria, con la condicionante de que el banco le restituirá cuando este lo requiera. Algo similar ocurre en los créditos rotativos de las tarjetas de crédito; a pesar que hay una disponibilidad de dinero cuando se hace efectivo, el traslado del mismo es cargado al usuario; en consecuencia, la titularidad del dinero, como bien fungible, está en función del usuario, que puede ser víctima de un delito de carácter informático.

Es preciso analizar ahora la obligación principal del banco por virtud del contrato en sí, es decir, analizar el derecho principal que ostenta el usuario. Con base en ello, se verificará qué régimen debe gobernar en los casos de *phishing:* si el general de obligaciones o el de responsabilidad.

Al respecto, primero se hará referencia a la naturaleza del depósito que realiza el usuario frente al banco. En este sentido, es pertinente traer a colación, la regulación propia del depósito voluntario regular e irregular que, por regla general, es el contrato, en que una de las partes entrega a la otra una cosa corporal o mueble para que la guarde y la restituya en especie a voluntad del depositante.

28 Marcos Rodríguez Puentes, "Responsabilidad bancaria frente al phishing" (Tesis de Maestría, Facultad de Derecho, Ciencias Políticas y Sociales Departamento de Derecho Bogotá, Colombia. 2015), 86.

Por tanto, las obligaciones del depositario son dos: custodiar la cosa y restituirla al depositante cuando este la solicite, esto quiere decir que las obligaciones del depositario son de custodia y de restitución. Sobre este punto, es importante el apartado anterior, en cuanto a establecer que la fungibilidad de los bienes trae a colación la restitución en otros de igual especie cuando estamos en presencia del depósito irregular.[29]

Ahora bien, esto lleva a un asunto adicional, referente a la cercanía del depósito irregular con el mutuo, toda vez que ambos implican la entrega de una cantidad específica de dinero cuya propiedad es transferida a quien la recibe, bien sea a título de mutuario o de depositario, a cargo de quien surge una obligación de restitución. Sobre este punto, el mutuo está referido a que cuando el banco entrega créditos rotativos al cliente, también entrega la titularidad del dinero; en consecuencia, el banco se despoja del dinero con la obligación del restituirlo al cliente,[30] con la supervisión del Estado, por la dualidad en la prestación de los servicios financieros a los que está obligado el banco.

Ahora bien, sobre estas premisas, tanto la institución financiera como el cliente están sujetos, en virtud del contrato de depósito irregular y créditos rotativos, a la restitución del dinero cuando operen las calidades de acreedor versus deudor; en los cuales, tanto banco como usuario pueden ostentar, dependiendo del tipo de operación (ya sea pasiva o activa).[31] En este sentido, cobra relevancia cuando el goce de los bienes los tiene un tercero de mala fe, que ha obrado para obtener de forma fraudulenta los bienes; en un primer momento debe de restituirlos el que teniendo la obligación de la custodia y resguardo los ha perdido, pero el problema está cuando existen excusas suficientes tanto para

29 *Cfr.* José Luis García Pita y Lastres, *El Derecho Bancario: Consideraciones Generales,* (Anuario de la Facultad de Derecho de la Universidad de da Coruña, 1999), 247. Las relaciones de organización del banco son internas, o establecen un vínculo con la Administración del Estado, que interviene sobre el sector económico de la actividad bancaria. Y otras son relaciones patrimoniales externas, establecidas con otros sujetos mediante la conclusión de contratos: De ahí que en el Derecho bancario debe de diferenciar una doble dimensión.

30 Marcos Rodríguez Puentes, "Responsabilidad bancaria frente al phishing" (Tesis de Maestría, Facultad de Derecho, Ciencias Políticas y Sociales Departamento de Derecho Bogotá, Colombia. 2015), 88.

31 Raquel López Ortega, *Las Operaciones Bancarias de Pasivo,* (Editorial Marcial Pons, España, 2008), 28.

el cliente como para el banco de obviar sus responsabilidades de restitución.

En ese sentido, el phishing es un problema tanto a nivel penal como civil, en el sentido que la restitución se vuelve un problema producto del perjuicio del delito, que lo paga quien tiene la obligación de restituirlo, pero también quien tuvo la pericia necesaria o guardó las providencias justas para responder frente al fraude, trasladando la responsabilidad al otro o, en su defecto, quien no expuso sus datos de forma voluntaria para ser defraudado.

Sobre este punto, en muchas ocasiones el consumidor financiero es confiado, imprudente y negligente en la gestión y prevención de los riesgos que se encuentran en su esfera de protección y cuidado, motivado por la falta de educación financiera, asimetrías en la información, falta de cultura, entre otras. En efecto, es usual que los clientes consumidores financieros compartan las claves con personas cercanas, que no guarden con celo su información financiera sensible, que no custodien adecuadamente los token para realizar operaciones, que no tengan los mecanismos de protección en equipos computacionales o smartphones o que abran, descarguen y sigan instrucciones falsas de correos sospechosos que anuncian premios, eventos o necesidades de información, para ser después objeto de saqueo de sus cuentas. Todas estas son circunstancias y hechos que multiplican el riesgo y viola las normas y obligaciones contractualmente asumidas por el consumidor y que, de presentarse un fraude, deben ser evaluadas por el operador jurídico al atribuir el grado de responsabilidad, para determinar si procede una restitución del dinero sustraído, ya sea de forma total, parcial, o ninguna.

Todas estas situaciones, modalidades y riesgos nos permiten afirmar que, en materia de sistemas para realizar operaciones electrónicas, existirán siempre dos órbitas de custodia y protección: la del banco en relación con la protección de sus sistemas operativos y la del consumidor financiero relacionada con el medio en el cual efectúan las transacciones y que, bajo las exigencias de la vida actual, debe tomar conciencia y adoptar conductas de autoprotección.[32]

32 Juliana Hernández Botero, "La Responsabilidad De Las Entidades Financieras Por Fraudes Electrónicos" (Tesis de Maestría. Escuela De Derecho Y Ciencias Políticas, Universidad Pontificia Bolivariana de Medellín, Colombia, 2020), 19.

Responsabilidad subjetiva, objetiva y responsabilidad compartida

Responsabilidad subjetiva

El régimen de responsabilidad subjetiva tiene su fundamento en la noción de "culpa", es decir, en la intención de inferir daño por parte de su causante o el grado de impericia o negligencia que genera tal daño. Así, el mecanismo principal para determinar la ausencia de responsabilidad por parte del causante del daño es la demostración de la diligencia que le es exigida en el caso particular, teniendo en cuenta que la responsabilidad contractual parte de presumir la culpa, se invierte la carga de la prueba y entonces no corresponde al titular del medio de pago probarla, sino al emisor acreditar su diligencia. Teniendo en cuenta, además, que la entidad financiera es un profesional en el desarrollo de su actividad, no está de más indicar que le corresponde un grado máximo de diligencia, por lo que responderá incluso de culpa levísima.

Sin embargo, teniendo como presupuesto el hecho de que la única fuente normativa de la relación jurídica entre el titular del medio de pago y su emisor es el contrato, que además es en la mayoría de los casos de adhesión, no es del todo sencillo acreditar que una de las obligaciones de la entidad financiera es brindar a sus clientes completa seguridad en la utilización de los medios electrónicos de pago.

De la misma manera, se debe partir del supuesto 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 todo resultado, pues trascendería entonces su obligación al ámbito de la responsabilidad objetiva. Todo lo expuesto permite concluir que los supuestos planteados no comprometen la diligencia del titular del medio de pago en su custodia, basta su manifestación en torno al incumplimiento contractual por parte de la entidad bancaria que derivó en el fraude electrónico, acreditando la causación y el monto de los

perjuicios, para que surja la responsabilidad civil como fuente de la obligación a cargo de la entidad bancaria de indemnizar los perjuicios, la que solo resultará indemne si acredita el mayor grado de diligencia.

Sin embargo, existe un evento que podría llegar a desvirtuar con argumentos prácticos lo hasta acá expuesto, en la cual es posible suponer que toda transacción u operación electrónica bancaria, realizada a través de un medio electrónico y validada por la contraseña del cliente, se entiende que efectivamente fue realizada por el mismo. Es evidente que, en esta hipótesis, por más pacto contractual que exista en torno a la obligación del emisor del medio de pago de brindar herramientas de seguridad a los clientes, bien sea de manera expresa o considerándolo como un elemento natural del contrato, basta para la entidad financiera indicar que la operación fue exitosa, pues se realizó con el medio de pago y su contraseña, que es el principal medio de seguridad brindado por el banco.[33]

Responsabilidad objetiva

En torno a las transacciones fraudulentas con cuenta y contraseña del titular es que surge la responsabilidad objetiva; es decir que surge dentro de la evolución del régimen de responsabilidad subjetiva, con la finalidad de equilibrar las cargas probatorias ante algunas circunstancias que resultaban ser, a todas luces, inequitativas.

Esta parte del supuesto que la responsabilidad de la entidad financiera es contractual y que no queda exenta de la misma ya que está obligada por la máxima diligencia en la gestión de la seguridad; sin embargo, se parte también de la teoría del riesgo bajo la órbita de la responsabilidad extracontractual por el incumplimiento de las obligaciones que estaban a cargo de la entidad financiera y por el riesgo generado de la actividad producida con los medios electrónicos. Por lo que, bajo ese supuesto, la entidad financiera está obligada a indemnizar al

33 Alejandro Rodríguez Zárate, "Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos: el riesgo provecho, el riesgo creado y el riesgo profesional", *Revista Universitas. N° 128.* Colombia, (2014): 294.

usuario por los perjuicios causados a este, ya que el riesgo es la posibilidad de la ocurrencia de una circunstancia que genere un perjuicio patrimonial al usuario.[34]

Por otra parte, es necesario sustentar la responsabilidad objetiva bajo la teoría del riesgo con pruebas periciales que acrediten esta por parte del banco y no por parte del usuario. Sin embargo, hay que recalcar que debido a que dicha responsabilidad no se encuentra fundada a nivel contractual, se considera que esto no impactaría en ninguna medida el hecho de haberse estipulado que cualquiera de estas transacciones se entienden realizadas por el titular del medio de pago. En otros términos, ya que el régimen de responsabilidad desborda de lo pactado, dejando de lado la diligencia de la entidad financiera y permitiendo estructurar su responsabilidad incluso en los eventos en que la operación sea realizada con el medio electrónico de pago y la contraseña fue dada a su titular, esto no significa que el banco no tenga ningún medio para quedar exento de responsabilidad,[35] pues puede hacerlo acreditando la fuerza mayor o la culpa exclusiva del cliente o de un tercero causante del perjuicio, es decir, rompiendo el nexo causal.[36]

34 *Cf.* Jorge Alberto Padilla Sánchez, y Mallory Zafra Sierra, "Responsabilidad de los establecimientos bancarios por el pago de cheques falsos o alterados en Colombia", *Revista de Derecho Privado. N° 32.* (2017): 400.

35 Juliana Hernández Botero, "La Responsabilidad De Las Entidades Financieras Por Fraudes Electrónicos" (Tesis de Maestría. Escuela de Derecho y Ciencias Políticas, Universidad Pontificia Bolivariana de Medellín, Colombia, 2020), 28. para exonerarse de responsabilidad, los bancos deben demostrar un incumplimiento del cliente y además acreditar el cumplimiento de obligaciones tales como: i) elaborar un perfil de costumbres transaccionales para cada cliente, que consiste en un análisis de las transacciones habituales realizadas por el cliente teniendo en cuenta los días, montos, destinatarios e incluso dirección IP desde la cual realiza habitualmente dichas operaciones, entre otros; ii) proceder con el bloqueo preventivo de la cuenta en caso de 29 advertir operaciones que no se adecuen al perfil transaccional del cliente. No basta con la notificación al cliente de las operaciones inusuales.

36 Alejandro Rodríguez Zárate, "Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos: el riesgo provecho, el riesgo creado y el riesgo profesional". *Revista Universitas. N° 128.* Colombia, (2014): 295.

Responsabilidad compartida

Al respecto, teniendo en cuenta que el banco mismo se pone en riesgo de sufrir fraudes al lanzar al mercado un mecanismo transaccional que puede ser de mucho o poco riesgo, según los niveles de seguridad del mecanismo, es necesario destacar que, ante cualquier ataque, es claro que siempre habrá culpa de la institución, y esta será determinante en la medida que los niveles de seguridad sean dependientes del riesgo asimilado.

En consecuencia, la culpa del usuario, de probarse en las condiciones legalmente exigidas, necesariamente concurrirá a la causación del perjuicio y no será exclusiva nunca, con la clarísima excepción del dolo; porque, en este caso, el perjuicio no provendría del riesgo propio del sistema, sino de la decisión del usuario malintencionado. Ahora bien, circunscribiéndonos al ámbito de la culpa, queda por ver qué tan viable es legalmente el reproche de las actuaciones del usuario; frente a lo cual, vale la pena mencionar que el usuario es responsable cuando se demuestra la no observancia de las buenas prácticas de seguridad.

Ante un evento de *phishing* el banco es la víctima, no el consumidor financiero, ya que la pérdida se da sobre el patrimonio de aquél y no de este, sin perjuicio de que el engaño que ha sufrido el banco y la automatización contable de la operación le lleva a inscribir en el registro del usuario la transacción de reembolso.

El presupuesto de desigualdad aplicado a la relación entre el usuario y el banco tiene dos efectos específicos: en primer lugar, que la negligencia capaz de generarle al banco el derecho de exigir resarcimiento por parte del usuario y compensar las obligaciones debe ser grave, pues no otra es capaz de generar en este ámbito una extinción de la obligación de restituir; en segundo lugar, que la carga de la prueba del pago y de la culpa grave del usuario corresponde al banco.

Finalmente, estas obligaciones se compensarían por parte del banco, con la consolidación sustantiva de la declaración contenida en la contabilidad en el sentido de que la deuda del banco se encuentra extinta, hasta concurrencia del fraude, sin perder de vista que la creación del riesgo y aprovechamiento del

riesgo por parte del banco, hacen que se trate siempre de culpas concurrentes. [37]

Conclusiones

1. El usuario o consumidor financiero responderá puntualmente por sus acciones, ya sean estas prudentes o negligentes, en los cuales exponga a terceros los datos de sus productos financieros o contraseñas solamente en casos de culpa grave; por hurto o estafa por medios informáticos. Por el contrario, la institución financiera, responderá de sus acciones ya sean estas prudentes o negligentes incluso por la culpa leve, por ser quien pone a disposición los mecanismos o tecnologías de la información a los clientes que se ven vulnerados, y porque esta debe de procurar los máximos estándares de seguridad en sus plataformas informáticas.
2. En el tema probatorio administrativo bancario, para determinar la culpa del usuario o consumidor financiero, ya sea grave o leve, la carga de la prueba para investigar y determinar los grados de responsabilidad le corresponde a la institución financiera, con la particularidad que está obligado al aviso pronto del fraude cometido al usuario o consumidor financiero y a la colaboración que debe de prestar; por otro lado, conforme a la investigación realizada por la institución financiera, deberá responder de forma total, parcial o negativa a la restitución del daño causado por los delitos financieros ocasionados por el *phishing*.
3. Corresponde tanto a la institución financiera como al consumidor financiero, denunciar, apoyar, y colaborar con las instituciones públicas encargadas de la persecución e investigación del delito, como Fiscalía General de la Republica, con auxilio de la Policía

37 Rodríguez Puentes, Marcos, "Responsabilidad bancaria frente al phishing" (Tesis de Maestría, Facultad de Derecho, Ciencias Políticas y Sociales Departamento de Derecho Bogotá, Colombia. 2015), 96.

Nacional Civil, a fin de individualizar al autor del phishing. y acreditar la existencia del delito, a fin de obtener una reparación tanto a nivel penal como civil, del daño sufrido no solo al patrimonio del usuario o consumidor financiero o banco, sino al colectivo en común.

Bibliografía

» Benavides Eduardo, Fuertes Walter, Sánchez Sandra. "Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura", *Revista Ciencia y Tecnología,* N° 13. (2020).

» Espinosa Sánchez Jesús Francisco. "Ciberdelincuencia. Aproximación criminológica de los delitos en la red". *La Razón histórica: revista hispanoamericana de historia de las ideas políticas y sociales. N°44,* (2019).

» García Pita y Lastres José Luis. *El Derecho Bancario: Consideraciones Generales,* (Anuario de la Facultad de Derecho de la Universidad de da Coruña, 1999).

» Hadnagy Christopher. *Ingeniería Social: El arte del hacking personal.* (Ediciones Anaya Multimedia, España, 2011).

» Hernández Botero Juliana. "La Responsabilidad De Las Entidades Financieras Por Fraudes Electrónicos". Tesis de Maestría. Escuela De Derecho Y Ciencias Políticas, Universidad Pontificia Bolivariana de Medellín, Colombia, 2020.

» Jiménez Orozco Genaro. "Distribución del Riesgo y Análisis de Responsabilidad en los casos de Fraude Informático bajo la modalidad de Phishing. Aplicación de la Ley de Protección y Defensa Efectiva del Consumidor". Tesis de Licenciatura. Facultad de Derecho de la Universidad de Costa Rica, 2012.

» López Ortega Raquel. *Las Operaciones Bancarias de Pasivo.* (Editorial Marcial Pons, España, 2008).

» Martínez Padilla Michel Paulina. *"La responsabilidad bancaria frente a los delitos informáticos".* (Tesis de Maestría, Universidad Andina Simón Bolívar. Ecuador. 2015).

» Oswaldo Ernesto Feusier Ayala. *Comentarios Generales sobre la Delincuencia Informática y la Ley Especial contra Delincuencia Informática y Delitos Conexos. Monográfico. Debates sobre el Sistema de Justicia Penal y Penitenciario.* (Consejo Nacional de la Judicatura, El Salvador, 2016).

» Oxman Nicolás. "Estafas informáticas a través de Internet". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, N° 41.* (2013).

» Padilla Sánchez Jorge Alberto y Zafra Sierra Mallory. "Responsabilidad de los establecimientos bancarios por el pago de cheques falsos o alterados en Colombia". *Revista de Derecho Privado. N° 32.* (2017).

» Puentes Marcos Rodríguez. "Responsabilidad bancaria frente al phishing". Tesis de Maestría, Facultad de Derecho, Ciencias Políticas y Sociales Departamento de Derecho Bogotá, Colombia. 2015.

» Rincón Arteaga Jaime et al. "Impacto económico y social del phishing y el smishing en Colombia y el mundo". *Revista Banca y Economía, Revista N° 1259,* (2020).

» Rodríguez Luna Víctor Manuel. Consult., *Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos.* (Fiscalía General de la República de El Salvador Escuela de Capacitación Fiscal, y Oficina de las Naciones Unidas contra la Droga y el Delito para Centroamérica y el Caribe, Sin Ed. 2018).

» Rodríguez Zárate Alejandro. "Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos: el riesgo provecho, el riesgo creado y el riesgo profesional". *Revista Universitas. N° 128.* (2014).

» Romero Castro Martha Irene et al. *Introducción a La Seguridad Informática y El Análisis de Vulnerabilidades.* (Universidad Estatal del Sur de Manabi, Ecuador, 1era Ed, 2018).

» Sain Gustavo, *Cibercrimen y delitos informáticos, los nuevos tipos penales en la era de internet.* (1ra Ed, Ciudad Autónoma de Buenos Aires: Erreius, 2018).