Universidad Andina Simón Bolívar

Sede Ecuador

Área de Derecho

Programa de Maestría en Derecho

Mención en Derecho Financiero, Bursátil y de Seguros

La responsabilidad bancaria frente a los delitos informáticos

Autora: Michel Paulina Martínez Padilla

2015

CLAUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN DE TESIS

Yo, Michel Paulina Martínez Padilla, autora de la tesis intitulada "LA RESPONSABILIDAD BANCARIA FRENTE A LOS DELITOS INFORMATICOS", mediante el presente documento dejo constancia de que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno de los requisitos previos para la obtención del título de Magíster en la Universidad Andina Simón Bolívar, Sede Ecuador.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Ecuador, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, durante 36 meses a partir de mi graduación, pudiendo por lo tanto la Universidad, utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en los formatos virtual, electrónico, digital, óptico, como usos en red local y en internet.

2. Declaro que en caso de presentarse cualquier reclamación de parte de terceros respecto de los derechos de autor/a de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y a la Universidad.

3. En esta fecha entrego a la Secretaría General, el ejemplar respectivo y sus anexos en formato impreso y digital o electrónico.

Quito, junio del 2015.

Firma: …….

UNIVERSIDAD ANDINA SIMON BOLIVAR

SEDE ECUADOR

AREA DE DERECHO

MAESTRIA EN DERECHO

MENCION EN DERECHO FINANCIERO, BURSATIL Y DE SEGUROS

La Responsabilidad Bancaria frente a los delitos informáticos

Autora: Michel Paulina Martínez Padilla

TUTORA: DRA. MARIA ELENA JARA

Quito, 2015

RESUMEN

La Superintendencia de Bancos y la Fiscalía General del Estado expidieron dos resoluciones interinstitucionales en el año 2011 por las que se obligó a las instituciones bancarias a reintegrar en favor de sus clientes, víctimas de delitos informáticos, determinados porcentajes de montos de dinero reclamado por ellos.

Para expedir las resoluciones se utilizaron una serie de argumentos desde el punto de vista constitucional, civil y del derecho del consumidor. En el ámbito constitucional se mencionó que las instituciones financieras son un servicio de orden público, mientras que en el ámbito civil se hizo referencia a la responsabilidad objetiva.

Luego de expedidas las resoluciones quedaron planteadas varios cuestionamientos sobre la legalidad de estas, de manera particular aquellos atinentes a si los bancos en efecto son un servicio de orden público y si, en realidad, en la relación contractual banco-cliente puede aplicarse la denominada responsabilidad objetiva, de acuerdo al ordenamiento jurídico ecuatoriano.

Este trabajo busca desentrañar varios términos utilizados en las resoluciones en mención para establecer su legalidad, previo a lo cual fue necesario analizar el tema de los delitos informáticos y las innovaciones incorporadas con referencia a éstos en el Código Orgánico Integral Penal, para determinar cuáles afectan a la banca y sus clientes.

Se hace referencia además en el trabajo a varia normativa expedida por la Superintendencia de Bancos mediante la que se dispone a los bancos tomar determinadas medidas para proteger a sus clientes contra el delito informático de apropiación ilícita de fondos.

TABLA DE CONTENIDO

LA RESPONSABILIDAD BANCARIA FRENTE A LOS DELITOS INFORMÁTICOS

INTRODUCCIÓN

La delincuencia crece a medida que se incrementan las tecnologías de la información, parecería así que mientras más medios tecnológicos aparecen en el mundo la delincuencia goza de más medios para cometer delitos y dispone de más víctimas.

En el presente trabajo se determina la responsabilidad de las entidades bancarias frente a sus clientes por el cometimiento de delitos informáticos, para lo cual he realizado un análisis de este tipo de infracciones diferenciando los distintos tipos penales que existen en nuestra legislación y determinando que dentro de su amplia gama el que nos interesa es el denominado fraude informático y dentro de éste el delito de apropiación ilícita de fondos por medios informáticos, incorporados en el Código Orgánico Integral Penal (COIP).

Por otra parte, al abordar el tema de la contratación bancaria y sus consecuencia legales es común hacerlo a la luz de los derechos del consumidor que si bien han sido citados en este trabajo, por cuanto no se puede prescindir de ellos para analizar el tema propuesto, no han sido desarrollados in extenso ya que he tratado de enfocarme en una perspectiva civil y penal por estar convencida de que la primera en mención es la que se tiene que aplicar con respecto al tema central que es la responsabilidad bancaria ante sus clientes frente al delito informático en el Ecuador.

En cumplimiento de los intereses propuestos he desarrollado el tema en dos capítulos: el primero para ubicarme en lo que se debe entender por “delito informático” e identificar cúal afecta a los usuarios de una entidad bancaria y dentro de éste, las diferentes modalidades por medio de las cuales el sujeto activo de este tipo puede defraudar tanto al banco como al usuario de éste. En el segundo capítulo analizo la

responsabilidad bancaria ante el cliente frente al delito informático de apropiación ilícita de fondos, dejando de manifiesto que aunque la entidad bancaria al igual que el cliente es víctima de éste, su responsabilidad se origina por el incumplimiento no solo de una obligación contractual sino de la obligación de las entidades bancarias de proveer las plataformas tecnológicas apropiadas para que sus clientes puedan acceder al servicio de banca en línea, concluyendo por tanto que dicha responsabilidad es subjetiva y no objetiva y que existen normas civiles que la rigen en la legislación ecuatoriana. Al finalizar el segundo capítulo analizo las resoluciones interinstitucionales 001 – FGE– SBS – 2011 y 002 – FGE – SBS – 2011 emitidas por la Fiscalía General del Estado y la Superintendencia de Bancos y Seguros, partiendo del análisis previo relacionado a la discusión de si las entidades bancarias prestan un servicio de orden público o no .

CAPÍTULO I

EL DELITO INFORMÁTICO QUE AFECTA A LA BANCA PRIVADA

1.1.- EL DELITO INFORMÁTICO.-

1.1.1.- Concepto y definición.-

El avance de la tecnología hace que la información mundial sea almacenada en computadores personales (PC), bases de datos, pendrives, información que a su vez es transmitida por medios de comunicación como el internet, cuyo uso hoy por hoy es infinito, incluso en el ámbito industrial, comercial, bancario. Cada vez entonces nos encontramos frente a un mayor desarrollo de la tecnología. El uso del internet permite que el mundo se mueva con mayor rapidez pero no con mayor seguridad ya que conforme el uso de éstos medios de comunicación avanza nos encontramos frente a conductas delictivas que buscan utilizar estos para cometer diversas clases de delitos.

Sin duda alguna la expresion "delitos informáticos" nos lleva a pensar en una computadora (hardware) y el un sistema (software) y en internet, que unidas a otros aditamentos hacen que se hable de las *Tecnologías de Información y Comunicación, denominadas TICS*[1], que son utilizadas por personas para cometer delitos que van desde el espionaje industrial hasta la pornografía infantil, pasando por delitos que atentan contra el patrimonio, que si bien forman parte de la amplia gama de delitos ya

[1] Las TICS son el conjunto de tecnología desarrolladas para transmitir información por medio de correos electrónicos, páginas web, mensajería instantánea, videoconferencias, etc.

estudiados por el Derecho Penal tienen un aditamento informático, de ahí que hay vertientes que admiten la existencia del delito informático y otras que la niegan manifestando que éstos no constituyen una nueva clase de delitos sino que simplemente son los mismos delitos ya tipificados en las legislaciones.

Entre los autores que aceptan la existencia independiente de delitos informáticos se encuentra el autor Jijena Leiva, quien los define como: "toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta la información contenida en los sistemas de tratamiento automatizado de la misma." [2] Los partidarios de la conceptualización independiente de esta clase de delitos los han dividido incluso en delitos informáticos y delitos computacionales, identificándoles a los primeros como aquéllos que afectan al soporte lógico de un sistema de procesamiento de información y los segundos como aquéllos que simplemente utilizan elementos de naturaleza informática para vulnerar bienes jurídicos reconocidos penalmente. [3]

Otros autores inadmiten la existencia de los denominados delitos informáticos, entre ellos se encuentran Viega Rodríguez y Bramont Arias, quienes manifiestan al respecto: "…los llamados delitos informáticos no constituyen una nueva categoría delictiva, sino que son los mismos delitos que ya se vienen castigando: delitos contra las personas, contra el honor, la libertad, la seguridad pública o la nación..." , mientras que el segundo nombrado expresa: "en realidad no existe un bien jurídico protegido en el delito informático porque no hay como tal un delito informático. Este no es más que una forma o método de ejecución de conductas delictivas que afectan a bienes jurídicos que ya gozan de una específica protección por el Derecho Penal".[4]

Enrique Rovira del Canto determina la existencia de los delitos informáticos realizando la siguiente clasificación: delitos no informáticos vinculados a la informática, delitos informáticos impropios y delitos informáticos propios. A continuación realizo

[2] Juan Vizueta Ronquillo, *Delitos Informáticos en el Ecuador*, Guayaquil, Editorial Edino, 2011, p.32.

[3] Ibidem.

[4] Juan Vizueta Ronquillo, *Delitos Informáticos en el Ecuador*, p. 31.

una síntesis del concepto de cada uno de éstos según lo propone el prenombrado tratadista:

Con referencia a los *delitos no informáticos vinculados a la informática*, Rovira del Canto, manifiesta que el comportamiento del agente activo del delito recae sobre elementos físicos informáticos (hardware) o que a pesar que se usa el sistema informático (software) no peligra la información, los datos o el sistema en sí [5], por ejemplo la pornografía infantil difundida por dichos medios. Por otra parte, en los *delitos informáticos impropios*, la utilización de los medios informáticos supone un quebranto a un bien jurídico tradicional pero además existe una afectación de la información en sí misma, al quebrantarse la seguridad y fiabilidad de un sistema informático,[6] por ejemplo la estafa utilizando propaganda falsa para que una persona realice una inversión en un negocio inexistente. Finalmente en cuanto a los *delitos informáticos propios*, éstos están relacionados con los comportamientos delictivos que por cualesquier medio tecnológico afecten la información y los datos informáticos en sí, concluyendo que en este tipo de delitos el bien jurídico protegido es la información, sin perjuicio de la consideración de otros bienes merecedores de protección conjunta, por ejemplo el crear una página web falsa de un banco con el propósito de que una persona crea que está ingresando a la real, siendo la finalidad de quien crea la página web falsa apropiarse de las claves de seguridad de un cuentacorrentista para transferir fondos de una cuenta a otra para apropiarse de fondos.[7]

En conclusión diremos que el delito informático siempre estará relacionado al uso, manipulación, apropiación de la información que forme parte de un sistema informático o de telecomunicaciones.

De manera personal, pienso que ante la disyuntiva de decidir si una determinada actuación constituye delito informático o no se debe atender al objetivo de la acción que

[5] Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos*, Granada, Editorial COMARES, 2002, pp. 130 a 132.

[6] Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos,* pp. 130 a 132

[7] Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos,* pp. 130 a 132.

obligatoriamente debe estar enfocada en la violación de información en el uso de medios informáticos como por ejemplo el internet. Ejemplifico lo dicho partiendo de un supuesto real: alguien por una red social anuncia que las personas pueden ganar dinero desde sus casas únicamente colocando publicidad de una determinada empresa en su red social facebook, prometiendo que por dicho trabajo cobrarán una remuneración pero que antes de acceder a este "negocio" deberán realizar una inversión de cincuenta dólares a ser transferidos a una cuenta bancaria. Este anuncio se publicita dos semanas en facebook y luego la cuenta desaparece sin que las personas sepan qué paso con el dinero que transfirieron. Este supuesto sería un delito pero no informático ya que si bien se está haciendo uso de medios tecnológicos no se está sustrayendo ninguna información ya que sus cuentas de facebook fueron utilizadas voluntariamente por las personas que creyeron en el negocio y que libremente depositaron el dinero requerido.

1.1.2.- Características.-

A continuación y de manera resumida determino las características de este tipo de delitos, según lo expone el autor Enrique Rovira del Canto:

a) La permanencia del hecho, en este tipo de delitos la acción para consumarlos generalmente es producto de una continua **repetición** hasta que el autor logra su objetivo, luego de lo cual éste continua con la comisión de actos ilícitos, lo que deriva en un *delito continuado*.[8]

   Sin embargo, el autor citado manifiesta, que en el evento que el sujeto activo del delito realice una acción inicial consistente por ejemplo en la manipulación del programa de funcionamiento informático, o un cambio en la base de datos, para que esa diversidad de acciones individuales mencionadas en el párrafo anterior provengan del "automatismo" del propio sistema, que repite automáticamente por sí mismo la manipulación, se podría considerar a este tipo de delitos también como "*delitos de consumación instantánea*".

b) Extensa y elevada lesividad, referente al daño económico , patrimonial y hasta a veces moral que causa a las víctimas.

[8] Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos,* pp. 77 – 79.

c) Dificultad en su averiguación y comprobación, debido al desconocimiento real del perjuicio producido, dado que en muchas ocasiones las víctimas son personas o corporaciones, por lo que se prefiere ocultar tales daños por la imagen de vulnerabilidad que puede representar.

d) La facilidad para encubrir el acto, por la tecnología usada en su comisión.

e) La disminución del riesgo de que el autor sea descubierto, debido a la posibilidad de borrar las huellas del delito.

f) Frecuencia y diversidad, dado que cada vez son más las personas que tienen acceso a internet y la diversificación del delito a la par de los avances tecnológicos, lo que hace que sean más peligrosos ante la reacción no siempre inmediata de los Estados desde el punto de vista jurídico y tecnológico.

g) Distanciamiento temporal y espacial, considerando que en este tipo de delitos la comisión del delito y la obtención del resultado no siempre es simultánea; en cuanto al espacio se considera que el autor puede estar distante del lugar en el que se materializa el hecho ilícito.

h) La transnacionalidad o el carácter fronterizo, ya que bien el delito se puede cometer en un país para que sus efectos tengan lugar en otro, en segundos, característica de la que nace la necesidad de concebir una legislación conjunta o supranacional que permita reprimir a esta clase de delitos.

i) En cuanto a los sujetos intervinientes en el delito, como sujeto activo es decir como autor se sitúa en la mayoría de casos a personas con conocimientos de informática, a profesionales de esta rama, a personas que trabajan en empresas que se dedican a esa actividad e incluso a empleados de confianza de las empresas afectadas que tienen acceso a dichos sistemas informáticos y conocen sus debilidades; atendiendo al tipo de delito que cometen. Así se habla de

hackers[9], crackers[10], cyberpunks[11], entre otros; mientras tanto los sujetos pasivos siempre van a ser personas que manejen un ordenador y en la mayoría de casos que tengan acceso a internet, que bien pueden ser titulares o beneficiario legítimos de un sistema informático o también usuarios permanentes o casuales de éstos.[12]

A parte de estas características se sitúa a otras como el alto nivel de tecnicismo, característica que se vincula con la alta dificultad de comprobación.[13]

1.1.3.- El Bien Jurídico Protegido.-

En atención a los derechos constitucionales protegidos y a la división de los tipos penales que protegen cada uno de estos derechos, el bien protegido en cada delito informático sería distinto atendiendo a la mentada división así, si hablamos de un delito informático de apropiación ilícita, el bien jurídico protegido sería la propiedad.

Sin embargo existen criterios coincidentes en establecer que el bien jurídico que protegen todos los delitos informáticos es *la información* mientras que otros hablan de la

[9] Son personas que buscan conocimiento e información contenida en bases de datos, su objetivo es violar seguridades, penetrar en forma no autorizada a sistemas de tratamiento de información, desmantelar los sistemas de seguridad con la finalidad de aumentar sus conocimientos o simplemente demostrar éstos al hacerlo.

[10] Son personas que buscan incomodar o dañar a otras, piratear software protegidos por leyes, destruir sistemas complejos mediante la transmisión de virus, denegar el servicio a usuarios legítimos, etc.

[11] Es la suma de dos palabras *cyber* y *punk*, que sirve para identificar a las personas que realizan las mismas actividades que los hackers empero lo hacen por rebeldía, intransigencia, cuestionar los establecido.

[12] Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos*, pp. 77 – 118.

[13] Al respecto el Dr. Diego Salamea, en su obra *El Delito Informático y la Prueba Pericial Informática*, p.35, manifiesta: "Una de las principales características de los delitos informáticos es su elevado nivel de tecnicidad, con clara incidencia en el ámbito probatorio, hecho que provoca una alta probabilidad de impunidad en la esfera de los delitos informáticos, según la visión de Reyna. La impunidad del delito informático no deriva exclusivamente de las dificultades probatorias que pueden generar conductas como ésta, muy tecnificadas".

libertad informática. A continuación cito dos autores que defienden cada una de estas posiciones.

La autora ecuatoriana Patricia Herrmann Fernández con referencia a la información como bien jurídico protegido en los delitos informáticos indica:

> "El Derecho Penal por ser un derecho sancionador sólo puede actuar cuando se pone en peligro o se lesiona un bien jurídico. ¿Pero que es un bien jurídico?. El bien jurídico según lo entiende la doctrina es siempre un interés vital, que no puede ser creado por el derecho sino por la sociedad de acuerdo a los valores vigentes en un tiempo dado.De acuerdo a esta noción hoy podemos afirmar que la información ha sido elevada a la categoría de un bien jurídico porque ha pasado a ser un interés jurídicamente protegido, que interesa a toda sociedad. Esa es la noción de bien jurídico que sostenemos. Un bien jurídico novedoso, complejo que puede tener implicancias en lo económico, en la privacidad, en la seguridad y en otros órdenes, pero que no deja de ser la información como objeto del delito."[14]

Santiago Acurio del Pino y Juan José Paez Rivadeneira, con referencia a la libertad informática sostienen:

> "En conclusión podemos decir que el bien jurídico protegido de acuerdo con nuestra Constitución es la llamada libertad de informática la misma que consiste, como expresión de la libertad del individuo, en el derecho de utilizar lícita y libremente, con los límites constitucionales y legales la tecnología informática. Esto esta dado en el reconocimiento de nuestra Constitución del acceso universal a las TICs por tanto a su uso libre."[15]

[14] Patricia Herrmann Fernández, *Comercio Electrónico*, Loja, Editorial de la Universidad Técnica Particular de Loja, 2006, p. 191.

[15] Juan José Paéz Rivadeneira y Santiago Acurio, *Derecho y Nuevas Tecnologías*, Quito, Corporación de Estudios y Publicaciones, 2010, p.210.

Sin embargo autores como Luis Bramont Arias Torres manifiesta que no existe un bien jurídico protegido en el delito informático porque este no es más que una forma o método de ejecución de conductas delictivas que afectan a bienes jurídicos que ya gozan de una protección específica en el Derecho Penal.[16] Siguiendo esta línea de pensamiento se establecen como bienes jurídicos protegidos: el patrimonio en el caso de ***fraudes informáticos***; la reserva y confidencialidad en el caso de delitos que afecten a la esfera de ***la intimidad***; la fe pública en el caso de las ***falsificaciones***. Autores como Claudio Magliona y Macarena López establecen que los delitos informáticos tienen el carácter de pluriofensivos o complejos porque "simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo"[17], afirmación con la que concuerdo.

1.1.4.- Clasificación.-

Saéz Capel, establece que: "la delincuencia mediante medios informáticos puede tener algunas especificidades, pero que éstas no son de tal naturaleza para crear nuevos tipos penales"[18].

El autor ecuatoriano Diego Salamea acota que "algunos autores clasifican al delito informático de acuerdo a la modalidad de comisión empleada", es decir de acuerdo al modo de cometimiento, por lo que realiza la siguiente clasificación del delito informático:

a) El fraude informático, consiste en la alteración y manipulación de datos y programas con una finalidad pecuniaria, en la mayoría de los casos.
b) El espionaje informático, obtención ilícita de datos y programas sin que media autorización del titular de éstos.

[16] Luis Bramont Arias Torres, *El Delito Informático en el Código Penal Peruano*, Biblioteca de Derecho Contemporáneo, Vol.6, p.58.

[17] Juan José Paéz Rivadeneira y Santiago Acurio, *Derecho y Nuevas Tecnologías*, p.211.

[18] Diego Salamea Carpio, *El Delito Informático y la Prueba Pericial Informática*, Quito, Editorial Jurídica del Ecuador, 2013, p. 22.

c) Sabotaje informático, destrucción o inutilización de un sistema. [19]

Téllez Valdez, citado por Rovira del Canto[20] diferencia entre lo informático como instrumento y lo informático como fin, realizando por ello la clasificación en:

a) Conductas que se valen de ordenadores como medio o símbolo en el cometimiento del delito;
b) Conductas que van dirigidas en contra del ordenador, accesorios o programas. [21]

Sin embargo es el mismo Rovira del Canto, el que realiza la siguiente clasificación que desde mi punto de vista resulta la más didáctica:

a) Infracciones a la intimidad.
b) Ilícitos económicos.
c) Ilícitos de comunicación por la emisión y difusión de contenidos ilegales y peligroso.
d) Otros ilícitos informáticos. [22]

1.2.- EL DELITO INFORMÁTICO EN LA LEGISLACIÓN ECUATORIANA.-

La introducción de los delitos informáticos en nuestra legislación tiene dos momentos importantes:

[19] Diego Salamea Carpio, *El Delito Informático y la Prueba Pericial Informática,* p. 24.

[20] Este autor en su obra ya citada, trae a colación en el tema de la clasificación de los delitos informáticos las realizadas por varios autores, sin embargo he citado las que me han parecido actuales. No por ello quiero dejar de mencionar que el autor mencionado como clasificación "tradicional" advierte que fue ***Lampe*** quien realizó la siguiente clasificación: 1.- manipulación de datos y/o programas, o fraude informático; 2.- copia ilegal de programas; 3.- espionaje informático; 4.- sabotaje informático; agresiones en el hardware o soporte material informático.

[21] Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos,* p. 123.

[22] Enrique Rovira del Canto, ob. cit, p.128.

a.- La expedición de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos publicada en el suplemento del Registro Oficial 557, de 17 de Abril del año 2002 marcó un hito histórico ya que por primera vez se reguló este ámbito. Uno de los aspectos innovadores fue la incorporación de las infracciones informáticas en el Código Penal, y

b.- La expedición del Código Orgánico Integral Penal – COIP- publicado en el Registro Oficial 180, de 10 de Febrero del año 2014, que conservó varios de los tipos introducidos al Código Penal en el año 2002 e introdujo nuevos tipos penales en lo que respecta a los delitos contra la propiedad que son los que nos interesa analizar en este trabajo.

Se debe precisar que en el año 2002, cuando se incorporaron mediante la Ley de Comercio Electrónico, Firmas y Mensajes de Datos los delitos informáticos en el Código Penal, ***no fueron ubicados ni en un capítulo ni en un título exclusivo*** sino que desde un principio fueron agregados a los capítulos y títulos referentes a distintos delitos ya existentes en nuestra legislación. Para entender lo manifestado he ubicado en la extinta norma penal los capítulos y títulos que fueron modificados mediante la incorporación en mención.

Fueron modificados: 1) Los delitos contra la *inviolabilidad de secretos*, que formaban parte del capítulo V del título **II** referente a los **DELITOS COMETIDOS CONTRA LAS GARANTÍAS CONSTITUCIONALES**; 2) Los delitos referentes a la *destrucción datos*, incorporados en el capítulo V del título **III** denominado **DELITOS CONTRA LA ADMINISTRACIÓN PUBLICA**; 3) Los delitos de *falsificación electrónica*, agregados al capítulo III, denominado falsificación documentos en general, que formaban parte del título **IV** alusivo a los **DELITOS CONTRA LA FE PÚBLICA**; 4) Los delitos de *daños informáticos al software*, añadidos al capitulo VII, denominado Incendio y otras destrucciones que se encontraban en el título **V** referente a **DELITOS CONTRA LA SEGURIDAD PUBLICA;** 5) Los delitos de *apropiación ilícita de información electrónica*, agregados al capitulo II denominado del Robo en el Titulo **X** titulado como **DELITOS CONTRA LA PROPIEDAD**; 6) *Otros delitos de apropiación ilícita* fueron incorporados a los delitos de Estafas y otras defraudaciones

contemplados al capitulo V del título **X** que llevaban el nombre de **DELITOS CONTRA LA PROPIEDAD**; 7) Además se introdujo *una contravención* informática de tercera clase referente a la violación al derecho de la intimidad en violación a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

El hecho de que a la fecha de realización del presente trabajo de investigación se haya publicado el COIP me releva de realizar un análisis de todos los delitos informáticos incorporados al extinto Código Penal en el año 2002, pero para fines didácticos en el ANEXO UNO he realizado un cuadro comparativo del texto de todos los delitos informáticos constantes en el Código Penal procurando ubicar los mismos en el texto actual constante en el COIP , cuadro en el que además ubico otros delitos relacionados con medios informáticos incorporados el último cuerpo legal en mención.

A diferencia del Código Penal en el COIP sí se ha realizado el intento de agrupar en una sola sección a este tipo de delitos. En efecto, en la sección tercera denominada "***Delitos contra la seguridad de los activos de los sistemas de información y comunicación***" del capítulo tercero (Delitos contra los derechos del buen vivir) del Título IV (Infracciones en particular) del COIP se encuentran ubicados la mayoría de delitos informáticos, aunque existen otros que si bien hacen alusión a tecnologías de información se encuentran dispersos en los distintos capítulos, así por ejemplo: en el Art. 173 se trata del delito del contacto con finalidad sexual con menores de dieciocho años por medios electrónicos contemplada en la sección cuarta (Delitos contra la integridad sexual y reproductiva) del capítulo II (Delitos contra los Derechos de Libertad) del Título IV. Dicho delito desde mi punto de vista sería un delito no informático vinculado a la informática.

En la elaboración del presente trabajo las infracciones que me interesan analizar son las referentes a los delitos contra la propiedad que afectan a los clientes y usuarios de la banca, para cuyo efecto realizaré una breve comparación entre los textos del Código Penal y del COIP, partiendo de lo contemplado en el primer cuerpo legal mencionado para luego ubicar dichos delitos en el segundo y determinar cómo éste varió.

1.2.1.- Delitos contra la propiedad.-

En el extinto Código Penal, se introdujeron los siguientes delitos informáticos en el capítulo V, que formaba parte del título X referente a los Delitos contra la Propiedad: delito de apropiación ilícita de información electrónica para facilitar la apropiación de bienes ajenos[23]; hurto o robo con variantes de uso de determinados dispositivos electrónicos[24]; y, la estafa electrónica[25].

En todos estos casos los bienes jurídicos protegidos eran el patrimonio de las personas y la información.

1.2.1.1.- La apropiación ilícita por medios electrónicos.-

El primer subtipo que contenía el artículo que trataba de este delito en el Código Penal era la *utilización fraudulenta* de medios de información o redes electrónicas para facilitarse un bien ajeno.

El denominado *verbo rector* del delito era utilizar fraudulentamente. Utilizar significa "emplear, usar, manejar, servirse, beneficiarse, disfrutar, gastar, consumir, aprovechar, dedicar, destinar, aplicar". El término fraudulentamente tal como consta utilizado se refiere a la intencionalidad que tiene el agente activo del delito.[26]

---

[23] **Art. 62**.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos in numerados: **Art. ...**- Apropiación ilícita (de información electrónica para facilitar apropiación de bienes ajenos).- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, ***o*** los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

[24] "**Art. 62**.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos in numerados: …**Art. ...**Pena por utilización de estos medios en hurto y robo.- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios: 1.Inutilización de sistemas de alarma o guarda; 2.Descubrimiento o descifrado de claves secretas o encriptadas; 3.Utilización de tarjetas magnéticas o perforadas; 4.Utilización de controles o instrumentos de apertura a distancia; y, 5. Violación de seguridades electrónicas, informáticas u otras semejantes."

[25] "**Art. 63**.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente: "Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos."

[26] Juan Vizueta Ronquillo, *Delitos Informáticos en el Ecuador*, Guayaquil, Editorial Edino, 2011, p. 83.

Los medios de los que se debía valer el sujeto activo eran los sistemas de información o redes electrónicas, definido el primero por la propia Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, como "todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar de cualquier forma, mensajes datos, mientras que las segundas como "el conjunto de equipos y sistemas de información interconectados electrónicamente". El autor Juan Vizueta Ronquillo establece la siguiente distinción entre unos y otros:

> "..los sistemas de información son medios por los cuales datos de importancia son compartidos de modo casi inmediato, entre personas o departamentos, utilizando para ellos diversas formas de comunicación; mientras que, la red electrónica de información es un conjunto de equipos y sistemas de información interconectados electrónicamente."[27]

El objetivo del delito era la apropiación de bienes ajenos.

El segundo subtipo era *procurarse la transferencia no consentida* de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

El verbo procurar significa intentar, pretender, esforzarse, acometer, emprender, empezar, tratar, proyectar, trabajar, proporcionar, facilitar, deparar, adquirir.

El objetivo era buscar una transferencia es decir pasar de un lugar a otro: bienes, valores o derechos de una persona, es decir bienes ajenos contra o sin el consentimiento del dueño. *Los verbos complementarios de la acción inicial* eran alterar, manipular, modificar, entendida la primera como el manejo manual y la segunda como la alteración

[27] Juan Vizueta Ronquillo, *Delitos Informáticos en el Ecuador*, p.84.

de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos, que deben existir previamente.

Los medios son los mismos que en el primer subtipo, el significado de *red electrónica* ya fue establecido mientras que el de *sistema informático* es definido por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos como "…todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar mensajes de datos"; *el programa informático* se refiere al software, *los mensajes de datos* es "toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio" según la mentada ley . *Los sistemas telemáticos* se refieren al uso de internet.

En los dos casos que contemplaba la disposición analizada la pena era de prisión de seis meses a cinco años.

En el *COIP*, la apropiación ilícita por medios electrónicos, se encuentra contemplada en el primer inciso del Art. 190, dentro de la sección Novena relativa a los Delitos contra el Derecho de Propiedad – Capítulo II – Título IV del Libro I, artículo cuyo texto es el siguiente:

> "Art. 190.-Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

Como vemos el delito materia de análisis no varía en su mayor parte en la redacción, es decir, recurre en la mayoría de términos que eran utilizados por el Código Penal, sin embargo en el COIP tiene variantes, las que por fines didácticos destaco en negrillas en el propio articulado que transcribo. Estas variantes son las siguientes:

a) Los medios de los que puede emplear el autor del delito no son solo los sistemas de información y las redes electrónicas sino también de telecomunicaciones y equipos terminales de telecomunicaciones.
b) Del texto del artículo se suprimió el término "mensaje de datos".
c) La pena mínima y máxima fueron modificadas, la primera de seis meses a un año y la segunda de cinco a tres años.

A parte del delito de *apropiación ilícita por medios electrónicos* se ha colocado en capítulo aparte del COIP el delito de *transferencia electrónica de activo patrimonial*, con lo que se busca proteger de la mejor manera a los clientes de la banca. [28]

1.2.1.2.- El hurto o robo utilizando dispositivos electrónicos.-

En el Código Penal, los delitos de hurto y robo podían ser castigados si se cometían: inutilizando sistemas de alarma o guarda; descubriendo o descifrando claves secretas o encriptadas; utilizando tarjetas magnéticas o perforadas; utilizando controles o instrumentos de apertura a distancia; y, violando seguridades electrónicas, informáticas u otras semejantes, mecanismos que no ameritan mayor análisis.

[28] Este delito se encuentra contemplado en el Titulo IV (Denominado Infracciones en general); Capítulo III (Delitos contra los derechos del Buen Vivir) Sección Tercera (Delitos contra la seguridad de los activos de los sistemas de información y comunicación). Dice así "**Artículo 231.- .- Transferencia electrónica de activo patrimonial.-** La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona."

En el COIP**,** el hurto y robo utilizando dispositivos electrónicos, se encuentra contemplado en el segundo inciso del Art. 190, dentro de la sección novena relativa a los Delitos contra el Derecho de Propiedad, Capítulo II, Título IV del Libro I, disposición que establece:

> "Art. 190.- …
> La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes."

La principal diferencia entre la redacción utilizada por el Código Penal y el COIP es que este delito ya no es tratado en un articulado independiente y que por tanto se ha borrado del texto enunciativo las palabras hurto y robo, por lo que, el que facilite la apropiación de un bien ajeno o el que procure la transferencia de bienes, valores y derechos, debe hacerlo del modo que describe el segundo inciso de la disposición.

1.2.1.3.- La estafa informática.-

En el caso de la "estafa informática" el Código Penal no definió lo que se debía entender por ésta, simplemente se limitó a establecer que en los casos de estafa utilizando medios electrónicos o telemáticos sería aplicable la pena máxima de la estafa, por lo que podemos decir, retomando lo que el mismo Código Penal decía del delito en mención, que la estafa electrónica es la apropiación de un bien ajeno llámese mueble, obligaciones, finiquitos, recibos; la que debe realizarse mediante engaños y en el caso específico que nos ocupa utilizando medios electrónicos o telemáticos.

En el COIP, no se habla de estafa cometida por medios electrónicos, sino que se precisa varios tipos de fraudes en el Art. 186, establecido la sección Novena relativa a

los Delitos contra el Derecho de Propiedad, Capítulo II, Título IV del Libro I, artículo que dice lo siguiente:

> **"Art. 186**.- Estafa.- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.
>
> La pena máxima se aplicará a la persona que:
>
> 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario
> 2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.
> 3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.
> 4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento
> 5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor…."

Los cinco numerales transcritos son sin duda alguna delitos que afectan a los usuarios de la banca, pero no por medios informáticos lo que evidentemente difiere del texto anterior del Código Penal que era más general al hablar de la estafa por medios "electrónicos o telemáticos"

La principal crítica que podemos formular al articulado transcrito es el hecho de que en muchos de los supuestos enumerados la estafa se podría dar mediante

falsificaciones ya que los términos utilizados nos llevan a una falsedad documentaria, entre ellos: “clonar” “duplicar” “certificación falsa” “transacciones ficticias”, por lo que consideramos no se debería juzgar como estafa sino como el delito en mención es decir como *falsificación*.

1.2.2.- Delitos contra la fé pública.-

1.2.2.1.- Falsificación Electrónica.-

En el Código Penal se encontraba tipificada en el capítulo III, denominado falsificación documentos en general, dentro del título IV , referente a los delitos contra la fe pública, dicha disposición establecía:

> "**Art. ...**- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:
> 1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
> 2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
> 3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
> El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo”.

La finalidad del cometimiento de esta clase de delitos no solo era el ánimo de lucro al igual que en los delitos de apropiación ilícita sino el simple interés de causar daño o perjuicio a un tercero configuraba el delito. El *medio* empleado podía ser

cualquiera. Las *formas de cometimiento* del delito eran la alteración; modificación; simulación; o suposición, todos verbos que suponen un cambio material de algo existente o la creación de algo parecido a lo que ya existe. El *objetivo* eran los mensajes de datos, anteriormente definidos.

Es importante distinguir que en la disposición transcrita se establecían tres tipos de falsedades:

La *falsedad material* contemplada en el numeral uno de la disposición transcrita, ya que el término *alterar* significa transformar un documento preexistente, en el caso que nos ocupa se hablaba de alterar mensajes de datos en alguno de sus elementos o requisitos de carácter formal o esencial; *el forjamiento* contemplado en el numeral dos, ya que la palabra simulación se la identifica con los términos fingir o imitar mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad y, en el numeral tres se trataba de suponer es decir colocar o considerar en un acto personas que no han intervenido en éste o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hicieron, lo que evidencia una *falsedad ideológica*.[29]

En el Código Integral Penal - COIP- este tipo penal ha sido suprimido, lo que desde mi punto de vista ha tratado de ser suplido con la creación de nuevos tipos penales empero creo que la falsedad es un tipo penal útil, con un ámbito amplio para proteger al agente pasivo del delito contra conductas delictivas.

1.2.3.- Los delitos contra la seguridad de los activos de los sistemas de información y comunicación, como innovación en el COIP .-

Para el trabajo que he desarrollado, la inclusión de este tipo de delitos en el COIP constituye una verdadera innovación.

Dentro de esta configuración novedosa que se ha establecido en la sección Tercera del Capítulo III relativo a los "Delitos contra los Derechos del Buen Vivir" del

[29] Juan Vizueta Ronquillo, *Delitos Informáticos en el Ecuador*, pp. 64 – 74.

Título IV denominado Infracciones en Particular del Libro I del COIP, se encuentran varios tipos penales identificados con los delitos informáticos que afectan a la banca, por lo que me remitiré exclusivamente a ellos.

> **"Art. 230**.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:
> 1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
> 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
> 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
> 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Del texto transcrito son los dos primeros numerales los que interesan a esta investigación en virtud que el primero hace alusión al phishing y el segundo al pharming, que son técnicas que se utilizan para afectar a los usuarios y clientes de la banca y de los que trataré de manera pormenorizada más adelante. Sin embargo, a mi criterio, a diferencia de los delitos que hemos analizado, no se establece el ánimo de lucro del autor del delito lo cual parecería una falencia ya que la mera alusión que se

hace a que el autor comete los delitos en provecho propio se presta a una serie de interpretaciones. De todas formas, es evidente que la intención del legislador es proteger la información y no el patrimonio quedando éste último bien jurídico resguardado con otras disposiciones ya analizadas, como es la contemplada en el Art. 190 del COIP.

En cuanto a los tipos descritos en los numerales tres y cuatro, luego del análisis realizado hasta el momento considero que no son propiamente delitos informáticos ya que no se manifiesta que su cometimiento se produzca utilizando sistemas o redes informáticas sino de otra forma.

Llama la atención, por otra parte, la incorporación de un delito que se asimila en extremo al delito de apropiación ilícita por medios informáticos establecido en el COIP y que ya fue materia de análisis. Creemos que en un afán de precautelar los intereses de los depositantes de la banca privada, lo que el legislador buscó es asegurar que ante su cometimiento no quede en la impunidad el hecho ilícito.

> **Art. 231**.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.
>
> Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona."

Como se puede apreciar en la disposición transcrita se utiliza los *mismos verbos* que en el Art. 190 del COIP: alterar, manipular modificar; el ánimo de lucro es también *la finalidad* del agente activo; *el medio* es cambiar artificialmente un programa o sistema informático o telemático, términos éstos utilizados en la mentada norma.

El objetivo del delito es facilitar una transferencia de activo patrimonial de una persona, que son bienes, valores y derechos.

Se castiga además a la persona titular de la información que haya revelado los datos de su cuenta bancaria a otra persona con la finalidad de suponer o aparentar una apropiación ilícita.

1.3.- MODALIDADES DE DELITOS INFORMÁTICOS QUE AFECTAN A LA BANCA QUE HAN SIDO RECOGIDOS POR EL CÓDIGO INTEGRAL PENAL.-

Del análisis que a continuación realizo se infiere que en el COIP se han tipificado delitos informáticos no solo buscando la protección de derechos constitucionales y bienes jurídicos conocidos tradicionalmente, como es por ejemplo el derecho a la propiedad, sino también el derecho de información, que se lo cataloga como un "derecho del buen vivir". En esta línea, los delitos que afectan a los clientes de la banca como a continuación analizo resultan no solo delitos contra la propiedad sino también delitos contra la información, ya que como se advertirá actualmente la simple interceptación de datos así no tenga el ánimo de lucro constituye delito. Esta idea no es nueva, como Rovira del Canto nos recuerda:

> "Los ilícitos informáticos en este campo se han venido considerando, por tanto, como delitos económicos, con todas sus características fundamentales comunes, incluido el elemento subjetivo del ánimo de lucro, en los que lo informático era el calificativo de aquéllos, atendidas, normalmente, *las peculiaridades de su medios comisivos y en cuanto afectaban a elementos no corpóreos: la información y los datos.*
>
> Sin embargo, en la estructuración actual de los delitos de riesgo informático y de la información, sobre la base de su caracterización y conceptualización en torno a los nuevos bienes jurídicos requeridos de protección jurídico penal (la información en sí misma, los datos informáticos, y la seguridad y fiabilidad en los sistemas informáticos y telemáticos), es al término actual

del delito informático a la que debemos aplicar el calificativo de económico, y no al revés, y que comprenden aquellos comportamientos ilícitos informáticos en el ámbito económico/patrimonial, y referirnos consecuentemente a los mismos como delitos informáticos económicos patrimoniales."[30]

Se infiere que cuando los delitos informáticos son cometidos con el ánimo de lucro se enmarcan dentro de los ilícitos económicos y cuando afectan al derecho de información podemos hablar de "otros delitos informáticos" siguiendo lo arriba manifestado por Rovira del Canto Rovira del Canto. Siguiendo la línea de pensamiento citada, en cuanto a los delitos que se cometen contra los clientes de la banca por medios informáticos pienso que si el agente activo de la infracción tiene el ánimo de lucro será un delito contra la propiedad y si no lo tuvo será un delito contra los sistemas de información como los llama actualmente el COIP.

Las modalidades conocidas para el cometimiento de delitos informáticos que afectan a los clientes de la banca han sido tipificadas en el COIP, según lo que a continuación analizo:

a) El *phishing***.-**

Según los autores ecuatorianos Juan José Paéz Rivadeneira y Santiago Acurio del Pino es el uso no autorizado que un tercero hace de los datos que identifican a una persona con el fin de defraudar o cometer otro delito con una motivación financiera. El delito consiste en obtener información tal como el número de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. [31], es decir que se trata de robarle parte de la identidad al sujeto pasivo.

[30] Enrique Rovira del Canto, *Delincuencia informática y fraudes informáticos,* p. 159.

[31] Juan José Paéz Rivadeneira y Santiago Acurio, *Derecho y Nuevas Tecnologías,* Quito, p.217.

Wilson Arcilla citado por Diego Salamea manifiesta: "Según lo describe la Unión Internacional de Telecomunicaciones el "phishing" es un acto que tiene por objeto lograr que la víctima revele información personal o confidencial. El término phishing se empleo inicialmente la utilización de los correos electrónicos para "pescar" (en inglés phish) contraseñas y datos financieros en un mar de usuarios de internet. El empleo de la grafía "ph" se relaciona con las convenciones terminológicas de uso común en la piratería informática."[32]

El Dr. Diego Salamea determina que para la realización del phishing se han creado incluso programas como el *spyware* direccionados a hurtar contraseñas que la persona digita en su computador y los *backdoors* que son virus creados para que el sujeto activo del delito ingrese directamente a la información que un computador tiene y revisar la información o bien puede venir en correos electrónicos no deseados, mensajes instantáneos de spam, solicitudes falsas de amigos. [33]

Como vimos, en el COIP este delito esta contemplado en el numeral uno del Art. 230.[34]

b) El *pharming*.-

Juan José Paéz Rivadeneira y Santiago Acurio del Pino, lo definen como un "ataque a los computadores personales que consiste en modificar o sustituir el archivo del servidor de nombres de dominio (D.N.S) cambiando el IP real de la entidad bancaria para que al escribir en la barra de direcciones el nombre de dominio de la entidad, el

[32] Diego Salamea Carpio, *El Delito Informático y la Prueba Pericial Informática*, p. 44.

[33] Diego Salamea Carpio, Ob Cit, p.58.

[34] "Art. 230.- Interceptación Ilegal de datos. Será sancionada con pena privativa de libertad de tres a cinco años: 1.- La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible".

navegador nos dirija a la dirección IP donde se aloja la página falsa de esa entidad en la que se recogerán claves de acceso de los clientes."[35]

En el pharming el sujeto activo del delito clona una página institucional como por ejemplo de un 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.

El pharming esta contemplado en el numeral 2 del Art. 230 del COIP.[36]

c) *La técnica del salami o Rounding of Utility***.-**

Consiste en redondear céntimos en determinadas operaciones bancarias para luego depositarlas en cuentas propias.[37]

Es una técnica especializada que también es denominada *técnica del salchichón* en otros lugares del mundo, en la cual rodajas muy pequeñas, apenas perceptibles, de transacciones financieras, se van tomando repetidamente de una cuenta y se transfieren a otra. Esta técnica consiste en introducir a los programas algunas instrucciones o condiciones para que envíe a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.[38]

Esta técnica se encuadra en la apropiación fraudulenta por medios electrónicos contemplada en el Art. 190 del COIP. [39]

---

[35] Juan José Paéz Rivadeneira y Santiago Acurio, *Derecho y Nuevas Tecnologías*, Quito, Corporación de Estudios y Publicaciones, 2010, p.218.

[36] "Art. 230.- Interceptación Ilegal de Datos. Será sancionada con pena privativa de libertad de tres a cinco años: …2.- La persona que diseñe, desarrolle, venda, ejecute, programe o envie mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder".

[37] Juan José Paéz Rivadeneira y Santiago Acurio, *Derecho y Nuevas Tecnologías*, p.215.

[38] Jefferson (único nombre que identifica al autor de la pagina) Artículo de Informática Forense, Técnica del Salami, http://jeffersonforense.blogspot.com/2011/08/delitos-informaticos-tecnica-del-salami.html. Revisado en Agosto del 2014.

[39] "Art. 190.-Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un

d) *Caballo de Troya*.-

Mediante la que se modifica las instrucciones a un programa informático ya existente, insertando nuevos programas o nuevas rutinas a fin de obtener resultados distintos a los previstos en la configuración inicial del programa para realizar una función no autorizada. [40].

Para el mejor entendimiento del concepto el Dr. Diego Salamea en la obra citada ejemplifica esta modalidad: "un caballo de troya informático entra en el sistema de forma aparentemente inofensiva (un archivo adjunto en un mail, un juego que te copia un amigo, un programa que te bajas de e Mule,…) y una vez dentro se activa, y se convierte en una herramienta, que, desde dentro, abre todas las puertas para que el atacante pueda tomar control total del sistema. ¡Un caballo de Troya, o troyano, permite incluso ver y escuchar al usuario del ordenador, sin que éste lo sepa!"[41]

Podría identificarse esta conducta a la contemplada en el numeral 2 del Art. 230 del COIP ya transcrito al pie de página cuando se trató del pharming.

e) El *hacking*.-

Se denomina así al acto de mero acceso o permanencia perpetrada con el fin de vulnerar un password o una puerta lógica que permite acceder a sistemas informáticos o redes de comunicación electrónica de datos. Se habla así del hacker blanco que es el sujeto que flanquea el acceso, accede al sistema informático y sale, con la finalidad de demostrar el fallo en la seguridad del mismo.[42]

---

bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años".

[40] Juan José Paéz Rivadeneira y Santiago Acurio, *Derecho y Nuevas Tecnologías,* p.214.

[41] Diego Salamea Carpio, *El Delito Informático y la Prueba Pericial Informática,* p. 83.

[42] Patricia Hermann Fernández, *Comercio Electrónico,* p.198.

En el COIP este delito podría encuadrarse en la figura descrita en el numeral uno del Art. 230 del COIP, ya transcrito al pie de página cuando se trató del pishing.

f) *El key logger*.-

El key logger comprende "herramientas de software o hardware que permiten grabar el texto que escribe una persona en su teclado. En el caso del software, el key logger captura todo lo que escribe la víctima y lo envía a una dirección de correo electrónico configurado por el delincuente. Estos programas se instalan y funcionan de manera "invisible" (no se da cuenta el usuario). Existen también unos dispositivos USB y PS2 que se conectan entre el PC y el teclado, los cuales graban en una memoria interna el texto tecleado en el computador."[43]

En el COIP este delito podría encuadrarse en la figura descrita en el numeral uno del Art. 230 del COIP, ya citado.

g) El *data diddling*.-

Que se origina mediante la introducción de datos falsos en los ordenadores o mediante la eliminación de informaciones veraces[44].

Esta modalidad también que consiste en la manipulación de datos de entrada al computador[45], el autor del delito realiza una manipulación del computador, sistema o red con la finalidad por ejemplo de que un comando del ordenador realice otra función para la que estaba prevista como el borrar archivos o crear identidades falsas, este es el tipo de técnica que se utiliza para derivar fondos de diversas cuentas a una cuenta determinada.

---

[43] Banco del Pacífico, página web, https://www.bancodelpacifico.com/servicio-al-cliente/servicios/seguridad.aspx. Revisado en Agosto del 2014.

[44] Juan Vizueta Ronquillo, *Delitos Informáticos en el Ecuador*, p.96.

[45] Juan José Paéz Rivadeneira y Santiago Acurio, *Derecho y Nuevas Tecnologías*, p.213.

En este caso estaríamos frente a una apropiación fraudulenta por medios electrónicos contemplada en el Art. 190 del COIP ya transcrito.

h) El *cloning o skimming* .-

Mediante los se duplican o clonan tarjetas, sin que tal hecho sea conocido por sus titulares valiéndose de terceras personas como por ejemplo de empleados de tiendas, a quienes los autores les proveen de artefactos electrónicos para copiar toda la información de la banda magnética.

Este delito en el actual COIP está contemplado en el numeral 3 del Art. 230.[46]

i) El *carding* .-

Este delito es cometido utilizando el número de una tarjeta de crédito existente, suplantando la identidad del titular de ésta con la finalidad por ejemplo de realizar compras on line. Como se advierte este delito tiene características de phishing.

En cuanto a la clonación como tal de una tarjeta de crédito, ésta configura el delito de estafa contemplado en el párrafo 3ro del Art. 186 del COIP.[47]

1.3.1- LA TECNOLOGÍA DE INFORMACIÓN COMO CAUSA PRIMARIA DEL RIESGO OPERATIVO EN LAS ENTIDADES BANCARIAS.-

El *fraude bancario* es un término que nace en Basilea II, a raíz del estudio del tema del riesgo operacional que fue conceptualizado como: "el riesgo de pérdida resultante de la insuficiencia o fallos de los procesos internos, las personas y los sistemas

[46] "Art. 230.- Interceptación Ilegal de Datos. Será sancionada con pena privativa de libertad de tres a cinco años: 3.- La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esta soportada en las tarjetas de crédito, debito o pago similares".

[47] "Art. 186.- ….La pena máxima se aplicará a la persona que: Defraude mediante el uso de tarjeta de crédito, debito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada u obtenida sin legítimo consentimiento de su propietario".

o de acontecimientos exteriores"[48], de ahí que puedan existir fraudes externos provenientes de personas que no laboran dentro de la entidad bancaria y fraudes internos, provenientes de personas que laboran al interior de ésta como por ejemplo la manipulación no autorizada en los sistemas informáticos. Son factores que inciden en el nivel de *riesgo operacional bancario*: el incremento de la utilización de tecnología y automatización de procesos; incremento de la complejidad de los productos; incrementos de las demandas de clientes; la proliferación de créditos, entre otros. El riesgo operacional es así un factor que para fines de la determinación de responsabilidad incumbe exclusivamente a la entidad bancaria, como generadora de éste, ya que es ésta quien a través de la oferta de productos la que debe precautelar que éste sea mínimo o nulo.

Para fines del análisis de los delitos informáticos que afectan a la banca, el estudio del riesgo operacional resulta determinante a fin de establecer si fue el Banco el que a través del cumplimiento de los lineamientos legales y directrices aminoró la existencia de este riesgo de tal modo que sus clientes y usuarios puedan acceder a un servicio seguro.

En el Ecuador, los lineamientos de Basilea se encuentran recogidos en el capítulo V denominado "De la Gestión del Riesgo operativo" del título X del Libro I de la codificación de resoluciones de la Superintendencia de Bancos y Seguros, incorporada mediante la resolución JB – 2005 – 834, la que contiene una serie de normativa que permite identificar, medir, controlar, mitigar y monitorear los riesgos derivados de fallas o insuficiencias en los procesos, personas, tecnologías de información y eventos externos. En el Art. 2.2 de la mencionada resolución, el evento del *riesgo operativo* se conceptualiza como todo *acontecimiento*, suceso, eventualidad o hecho imprevisto que puede ocasionar pérdidas económicas para la institución controlada, los mismos que pueden provenir de factores del riesgo operativo: "fraudes internos; fraudes externos; prácticas laborales y seguridad del ambiente del trabajo; practicas relacionadas con los

[48] Francisco Alvarez Valdez, Fraudes *Bancarios. Impacto en el resto de las Entidades del Sistema Financiero* , Mitigación del Riesgo y Sanciones Aplicadas, XXIX Congreso Latinoamericano de Derecho Financiero, 2010. http://www.felaban.com/archivos_actividades_congresos/11.pdf.

clientes, los productos y el negocio; daños a los activos físicos; interrupción del negocio por fallas en las *tecnologías de información*; deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros", según enumera el Art. 2.3 de la resolución.

Se infiere que uno de los "factores" del riesgo operativo constituye la *tecnología de la información*, entendida esta en el Art. 2.15 de la norma legal citada como "el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información, incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados entre otros".[49]

La complejidad del factor de *tecnologías de la información* se debe a que requiere abarcar a todos los estamentos de la institución e implica un tecnicismo muy alto. No solo se trata de ayudar al funcionamiento de la entidad sino que bajo parámetros internacionales blinde sus sistemas para brindar un servicio confiable.[50]

En lo que respecta a los fraudes informáticos, la Junta Bancaria mediante Resolución JB – 2012 – 2148 expidió una serie de normativa que incluye acciones que debían ser implementadas por las instituciones del sistema financiero para mitigar el riesgo de fraude por el uso de tecnología de información y comunicaciones, en ésta encontramos regulaciones referentes a la banca electrónica y a las seguridades que debían adoptar las entidades bancarias al respecto de ésta, entre otros aspectos.

[49] Ecuador, Junta Bancaria, resolución JB – 2005 – 834.

[50] Deloitte, Riesgo Operativo, Resolución JB-2005-834, Estamos Listos? http://www.deloitte.com/view/es_ECcc/perpectivas/estudios-y-publicaciones/articulo.

CAPíTULO II

LA RESPONSABILIDAD BANCARIA FRENTE AL DELITO INFORMÁTICO

2.1.- LA ACTIVIDAD BANCARIA COMO SERVICIO DE ORDEN PÚBLICO.-

Previo analizar los distintos tipos de responsabilidad de la banca, es preciso partir de la conceptualización que hoy por hoy se le ha dado al servicio bancario.

El Art.- 308 de la Constitución de la República establece:

> "Art. 308.- Actividades, finalidad, prohibiciones y responsabilidad del sistema financiero.- Las actividades financieras son un *servicio de orden público* y podrán ejercerse previa autorización del Estado, de acuerdo con la ley; tendrán la finalidad fundamental de preservar los depósitos y atender los requerimientos de financiamiento para la consecución de los objetivos de desarrollo del país. Las actividades financieras intermediarán de forma eficiente los recursos captados para fortalecer la inversión productiva nacional y el consumo social y ambientalmente responsable.
>
> El Estado fomentará el acceso a los servicios financieros y a la democratización del crédito. Se prohíben las practicas colusorias, el anatocismo y la usura.
>
> La regulación y el control del sector financiero privado no trasladarán la responsabilidad de la solvencia bancaria ni supondrán garantía alguna del

> Estado. Las administradores y administradoras de las instituciones financieras y quienes controlen su capital serán responsables de su solvencia. Se prohíbe el congelamiento o la retención arbitraria o generalizada de los fondos o depósitos en las instituciones financieras públicas o privadas."

La utilización de las palabras "servicio" y "de orden público" sin duda fue una innovación de la Constitución expedida en el año 2008.

El término ***servicio***, implica un conjunto de actividades que busca responder a las necesidades de la gente, pero si le aumentamos a esta palabra el término "público" obviamente nos viene a la mente que esta actividad debe nacer, desarrollarse y regularse por el Estado. El ***servicio público*** así es "aquella actividad del Estado para la realización de un fin, considerado por los gobernantes de interés general."[51]

Según el autor Enrique Rojas Franco, el servicio público tiene dos sentidos uno orgánico, que es la actividad que realiza una institución pública y otro material, que es la manera como esa actividad se realiza, de ahí que puedan existir organismos que presten servicios públicos pero que no necesariamente sean de origen estatal, dice el autor mencionado: "cuando un órgano privado tiene una misión de servicio público implica que la dirección, ejecución, funcionamiento y responsabilidad con motivo de la ejecución de ese servicio, es por cuenta del organismo privado y no del Estado, el cual lo único que podrá hacer eventualmente es controlar la actividad del órgano privado."[52]

Marienhoff distingue servicios públicos propios y servicios públicos impropios. El primero es el prestado por el Estado directamente o indirectamente por un concesionario. El impropio es el prestado por personas privadas, de acuerdo a disposiciones reglamentarias establecidas por la Administración Pública. El elemento

[51] Enrique Rojas Franco, *Derecho Administrativo y Derecho Procesal Administrativo*, Guayaquil, Edilex S.A., 2007, p.189.

[52] Enrique Rojas Franco, *Derecho Administrativo y Derecho Procesal Administrativo*, p.191.

público, dice este autor, no se refiere al ente que lo presta sino al destinatario, por lo que el servicio público no es otra cosa que servicio "para" el público. [53]

La Constitución expedida en el año 2008 no trata al servicio de intermediación financiera como un servicio público sino de **"orden público**", que desde mi punto de vista obedece a simple forma ya que con la reforma introducida es innegable que lo que se quiso decir es que estas actividades constituyen un servicio público, aunque en un determinado momento se justificó el uso de dichos términos argumentando que el considerar a dichas actividades como de orden público se refería a la autorización por parte del Estado que requiere una entidad bancaria para su funcionamiento y control, esta postura de intervencionismo estatal ha sido justificada del siguiente modo:

> "El intervencionismo se concreta, en lo que se refiere al aspecto normativo, en un conjunto de disposiciones que estructuran el sistema bancario, en lo relativo a su organización y regulación, así como también en un conjunto de normas referidas a ciertas obligaciones que las entidades deben observar en su contratación con los clientes. Tal intromisión se justifica, para algunos autores, sólo porque la banca satisface necesidades de la comunidad, lo cual en su conjunto, según como esas actividades se lleven a cabo, afectan el interés general."[54]

Al respecto de la utilización del término "***orden público***" para referirse a las actividades del sistema financiero en la Constitución de la República, la Asociación de Bancos Privados del Ecuador, realizó la siguiente observación:

> " El "Orden Público" es uno de aquellos que la doctrina denomina como "conceptos jurídicos indeterminados", tales como la "buena fe", el "buen padre de familia", etc. Su delimitación por lo tanto no es sencilla, sin embargo éste -el orden público- de manera genérica, de acuerdo a la doctrina mayoritaria, no supone sino la sujeción estricta a la normativa

[53] Grando Jose y Medina Marcos. UNIVERSIDAD NACIONAL DEL NORESTE. *Comunicaciones Científicas y Tecnológicas* 2006. Facultad de Derecho y Cs. Sociales y Políticas (UNNE). Salta Nº 465- Código Postal 3400 – Corrientes Capital – República Argentina. http://www.unne.edu.ar/unnevieja/Web/cyt/cyt2006/01-Sociales/2006-S-066.pdf.

[54] Eduardo Antonio Barbier, *Contratación Bancaria, Buenos Aires*, Editorial Astrea, 2000, p.39.

> que rige determinada actividad, es decir implica que las disposiciones emitidas que regulan un servicio no son disponibles para las partes, siendo entonces mayor la potestad de regulación del Estado sobre el mismo. Es decir la caracterización de orden público recoge lo que se espera de la regulación estatal sobre la actividad bancaria, no así la noción de servicio público."[55]

Se infiere entonces que el objetivo que tuvo la Asamblea Constituyente en el año 2008 fue no solo crear el ambiente propicio para que los organismos de control tengan un mayor poder de regulación sobre la banca privada, que siempre lo han tenido, sino además que respondan a las necesidades de las personas pero del modo que el Estado lo proponga.

Por otra parte, se debe establecer que existe servicio público únicamente cuando la ley así declara a una actividad.

> "Así, según la mayor parte de autores de nuestro medio, hay servicio público únicamente cuando una ley así lo declara a una determinada actividad, mediante una calificación formal y específica, que importa su publificación (*publicatio*).Esto trae aparejado la asunción formal de la titularidad estatal de la actividad publificada, que implica a su vez qu la misma pase a formar parte de los cometidos materiales pertenecientes a la función administrativa de la Administración Pública."[56]

Las connotaciones que acarrea que una actividad sea declarada como servicio público, son entre otras: a) La administración pública pasa a ser el titular del servicio, por lo que los particulares no pueden desarrollarla, a menos que exista una expresa delegación que no debe tener el carácter de permanente y bajo los parámetros

---

[55] Asociación de Bancos Privados del Ecuador, ¿Los servicios Financieros, un servicio público?, Boletín Informativo Nro 37, 2014, http://www.asobancos.org.ec//ABPE_INFORMA/No37.PdF. Revisado en Agosto del 2014.

[56] Lucas A. Piaggio, *La Banca como servicio público - una ficción legal contra natura*, Federación Latinoamericana de Bancos , FELABAN, 2010, p. 17 – 33. Revisado en Agosto del 2014.

establecidos por el Estado, pudiendo por tanto darse la reversión de ésta; b) El servicio debe ser prestado con regularidad, continuidad, igualdad y obligatoriedad, características propias de todo servicio público; c) los precios o tarifas de los productos y servicios que ofrece quien desarrolla un servicio público se encuentran regulados por el Estado, quien debe además aprobarlos.

Los opositores a considerar las actividades financieras como un servicio público establecen que la banca no se ajusta a tal naturaleza en atención a las características establecidas en los literales b) y c) del párrafo anterior ya que a pesar de ser un servicio controlado por el Estado no siempre es continuo; no es igualitario ya que en la realidad la banca que ejerce actividades financieras hacen diferenciación en el tratamiento de sus clientes y no puede ser obligatorio ya que no se le puede obligar a la entidad bancaria a celebrar contratos con todas las personas que lo requieran, concluyendo así que el colocar a las actividades financieras como un servicio público atenta contra los cimientos de dicha actividad concebida como una actividad privada en la que existe un interés público o general. [57]

La importancia de discernir si la banca presta o no un servicio público se refleja en las consecuencias que ello acarrea en cuanto a la determinación de responsabilidades, ya que si asumimos que el servicio de intermediación financiera es un servicio público, la Constitución de la República determina al respecto en su Art. 54, referente a los derechos de las personas usuarias y consumidores, lo siguiente: "Las personas o entidades que presten servicio público o que produzcan o comercialicen bienes de consumo, **serán responsables civil y penalmente** por la deficiente prestación del servicio, por la calidad defectuosa del producto, o cuando sus condiciones no estén de acuerdo con la publicidad efectuada o con la descripción que incorpore.."

Me corresponde a continuación analizar la responsabilidad civil y penal de los bancos, no necesariamente desde el punto de vista de la Ley Orgánica de Defensa del Consumidor sino desde los ámbitos civil y penal, adentrándome en una visión que busca

[57] Lucas A. Piaggio, *IBidem*; pp. 17 – 33, Revisado en Agosto del 2014.

establecer cuáles son los mecanismos adecuados a utilizar por parte del cliente bancario frente al delito informático.

2.2.- RESPONSABILIDAD CIVIL DE LA BANCA.-

El autor Carlos Gilberto Villegas al respecto de lo que significa el término responsabilidad, manifiesta: "la imputación de una sanción a una conducta antijurídica que provoca perjuicios, es decir es la consecuencia (sanción) que la ley establece con motivo de una actuación humana voluntaria violatoria de la norma jurídica (sea la norma general o la norma particular) generadora de un perjuicio a otra persona"[58]

Del concepto anotado se infiere los elementos sobre los que se basa la responsabilidad bancaria, al igual que los otros tipos de responsabilidades : a) la antijuridicidad que requiere la existencia de un acto o un hecho humano, doloso o culposo, contrario a la ley o a un contrato, en otras palabras y en materia civil: la culpa; b) el daño económico o perjuicio a los bienes o derechos de una persona; y, c) el nexo causal entre antijuridicidad - culpa y perjuicio, de modo que entre uno y otro exista una relación de causa y efecto.[59]

La responsabilidad civil de los bancos nace del principio de tutela reparatoria o resarcitoria frente al perjuicio sufrido como producto de la culpa de la entidad bancaria frente a un detrimento patrimonial de sus clientes y usuarios de ésta:

> "..la tutela del cliente bancario relativa, en líneas generales, a la protección de derechos creditorios, merece ser abordada desde la perspectiva de la tutela resarcitoria, pero en subsidio de la tutela preventiva y coercitiva, de modo que aquella protección más débil sea compensada adecuadamente, no ya en ocasión de la reparación sino para evitar llegar a ella.

[58] Carlos Gilberto Villegas, *Contratos Mercantiles y Bancarios*, Tomo II, Buenos Aires, Su Gráfica, 2005, p.130.

[59] Eduardo Antonio Barbier, *Contratación Bancaria, Buenos Aires*, Editorial Astrea, 2000, p.527

> La reparación es, sin duda, el remedio último para restablecer el equilibrio – aun reconociendo un cierto desequilibrio congénito atribuible al margen de beneficio que orienta las relaciones patrimoniales-, ya que procura reubicar a las partes en la misma situación en la que se hubieren encontrado de no haberse generado un daño." [60]

La determinación de la culpa se establece según las reglas del Código Civil, diferenciando entre culpa contractual y extracontractual; originándose la primera en el caso que nos ocupa en los daños ocasionados por los bancos a sus clientes por el elemento contractual que los une, es decir cuando entre las dos partes banco – cliente se ha suscrito un contrato por el cual el primero oferta al segundo servicios de banca el línea; mientras que la segunda se origina por los daños sufridos sin que medie una relación contractual, por delitos o cuasidelitos, lo cual se origina ante la inexistencia de una relación previamente convenida como es el caso de los usuarios de la banca que sufren un daño sin ser clientes de ésta, como se analizará con posterioridad.

Los eximentes de responsabilidad civil son la culpa de la víctima, el caso fortuito o la fuerza mayor, y el hecho de un tercero, éste último solo en los casos de la responsabilidad contractual ya que se entiende que en el caso que se suscite dicha actuación y se compruebe que el hecho realizado por el tercero fue *la única* causa del perjuicio, funciona como una causal de responsabilidad civil. [61]

En esta parte es importante establecer que tanto en la responsabilidad contractual como en la extracontractual el daño debe ser ocasionado al cliente bancario, entendido éste según el siguiente concepto:

> "Clientes no son solo quienes realizan determinadas operaciones con las entidades, como equivocadamente se ha sostenido en alguna ocasión, sino cualquier persona, física o jurídica que utiliza alguno de los servicios que presta una entidad financiera: quien cobra un cheque o un giro, quien

[60] Eduardo Antonio Barbier, *Contratación Bancaria*, p.525.

[61] Marianna Fonseca Villanea, *El hecho de un tercero como eximente de la responsabilidad objetiva bancaria*, http://www.ulacit.ac.cr/files/careers/48_fonsecavillanea.pdf.

efectúa un depósito a la vista o a plazo, quien confía un mandato o una cesión, quien sin concertar ninguna operación realiza una manifestación de bienes ante la entidad, quien recibe y cobra una transferencia, el titular de un crédito etcétera. Todas esas personas tienen necesidad de que esos hechos y operaciones se mantengan en reserva, y así debe ser."[62]

Por su parte, el Código de Derechos del Usuario del Sistema Financiero, en el glosario de términos establece: "Usuario del Sistema Financiero.- Persona natural o jurídica que hace uso de los servicios y productos de las instituciones del sistema financiero, pudiendo hacerlo de manera directa o indirecta."[63]

Se infiere que el término *cliente bancario* no es solo aplicable a quienes hayan celebrado un contrato con la entidad bancaria sino otro tipo de usuarios, conforme se estipula en la resolución Nro. JB – 2009 de 31 de Marzo del 2009 que incorporó la figura del Defensor del Cliente de las Instituciones Públicas de los sectores financieros público y privado, en cuyo glosario encontramos la siguiente definición de cliente concordante con la establecida en el Código de Derechos del Usuario del Sistema Financiero: "Es la persona natural o jurídica, sociedad de hecho o de derecho con la que una institución de los sectores financieros público y privado establece, de manera directa o indirecta, ocasional o permanente, una relación contractual de carácter financiero, económico o comercial. La condición de cliente será acreditada con la sola presentación de cualquier documento que acredita la existencia de una relación contractual entre éste y la institución financiera."

Los bancos son responsables ante sus clientes por los contratos que celebran con ellos, por lo que responden por la inejecución o defectuosa ejecución de las operaciones a las que se compromete; pero también es responsable ante sus usuarios por los actos efectuados por sus dependientes. [64] Al igual que en las otras especies de contratos, y como lo analizaré más adelante, la responsabilidad originada en el incumplimiento de

[62] Eduardo Antonio Barbier, *Contratación Bancaria*, p.62.

[63] Ecuador. Resolución JB – 2010 – 1782.

[64] Carlos Gilberto Villegas, *Contratos Mercantiles y Bancarios*, Tomo II, p.131

obligaciones que nacen de un contrato supone la presunción de culpa del deudor o agente dañoso, y por ende la carga de la prueba recae sobre éste.

En el ámbito de la responsabilidad contractual, es decir aquella que nace de un contrato, resulta interesante el tema atinente a las cláusulas contractuales que limitan o eximen la responsabilidad de los bancos. Al tratarse de contratos de adhesión por disposición del Art. 43 de la Ley Orgánica de Defensa del Consumidor, es expresamente prohibido la utilización de cláusulas eximentes de responsabilidad, ya que tal norma establece: "Son nulas de pleno derecho y no producirán efecto alguno las cláusulas o estipulaciones contractuales que: 1.- Eximan o limiten la responsabilidad de los proveedores por vicios de cualquier naturaleza de los bienes o servicios prestados", circunstancia que debemos tener en cuenta para el análisis que se realizara más delante de los contratos bancarios denominados *servicios en línea*.

Tanto en la determinación de la responsabilidad contractual como de la extracontractual, debe considerarse los criterios de imputación relacionados con la *responsabilidad subjetiva y objetiva*, diferenciación que se la realiza en atención a la pregunta: ¿Por qué una persona determinada y no otra es la que debe resarcir a la víctima?.[65]

La responsabilidad civil subjetiva es "la responsabilidad civil tradicional, conocida por la doctrina desde épocas remotas y estructuradas desde los tiempos de Roma, según la cual sólo deben ser reparados los daños que el agente cause por su propia culpa. Si el agente que causa el daño no incurrió en culpa al ocasionarlo, debe quedar exonerado de la reparación. Sólo existe responsabilidad civil si el agente procede

[65] Sobre los orígenes de la distinción de la responsabilidad subjetiva de la objetiva, se establece que en el Derecho antiguo se tenía una noción objetiva de la responsabilidad, bastaba así que una persona sufriera el daño para que tuviera el derecho a una reparación, noción que se fue abandonando poco a poco y que fue sustituida por la responsabilidad subjetiva, que exigía la existencia de la culpa o dolo por parte del autor del daño, doctrina que fue acogida por el Código Francés y aceptada por el Código Civil Chileno en el que el ecuatoriano se basó.

con culpa. La responsabilidad civil depende de la condición subjetiva de actuación culposa."[66]

Del concepto transcrito tenemos que para la determinación de la *responsabilidad subjetiva* debe probarse: a) la existencia del daño o perjuicio imputable a un sujeto determinado; b) la existencia de la culpa; y, c) una relación de causalidad entre el hecho y el daño generador, es decir que la actuación de un sujeto es lo que provocó el daño.

A continuación, analizaré brevemente cada uno de los elementos arriba descritos:

El daño es la lesión de un derecho que se trasluce en una merma patrimonial o en un padecimiento moral[67]. Dentro de esta concepción se diferencia el daño material del daño moral, el primero existirá siempre que se cause a otro un perjuicio susceptible de apreciación pecuniaria, ya que es ocasionado al patrimonio material de la víctima. El daño material con menoscabo del patrimonio material en sí mismo, puede dividirse en daño emergente y lucro cesante, el primero es la pérdida o disminución de valores económicos ya existentes, con un empobrecimiento del patrimonio, el segundo implica la frustración de ventajas económicas esperadas, o sea, la pérdida de ganancias de las cuales se ha privado a la persona que lo sufre. El daño moral es todo sufrimiento o dolor que se padece independientemente de cualquier repercusión de orden patrimonial material, es la lesión a las afecciones íntimas del damnificado.[68]

La culpa es un estado reprochable a un determinado sujeto[69], es la conducta contraria al deber de prevenir las consecuencias previsibles. Pero si bien no existe el propósito previsible de causar daño, alcanza igualmente el resultado negativo por no

---

[66] Temas de Derecho, *La Responsabilidad Civil*, http://temasdederecho.com/2012/06/04/la-responsabilidad-civil/. Revisado en Marzo del 2015.

[67] Jaime Mendieta, La culpa *incontrahendo – Historia, Evolución y Estado Actual de la cuestión*, http://www.emercatoria.edu.co/PAGINAS/VOLUMEN10/HTML2/125.html. Revisado en Noviembre del 2014.

[68] Ecuador. Corte Suprema de Justicia, (Sentencia de casación: *Caso Delfina Torres vs PetroEcuador*, expediente número 229 – 2002), publicado en el R.O. Nro.43 de 19 de marzo del 2003.

[69] Ramón Daniel Pizarro, *Responsabilidad Civil por el Riesgo o Civil de las cosas*, Buenos Aires, Editorial Universidad, 1983, p.52.

haber tenido el sujeto el cuidado de adoptar las medidas necesarias para impedirlo. La culpa y el dolo se asemejan en cuanto los dos causan daño.

Es importante señalar que en las obligaciones contractuales existe una presunción de existencia de culpa, no así en las extracontractuales en la que quien pretende la reparación tiene que acreditar que ha habido culpa de parte del deudor.[70]

La *relación de causalidad entre la culpa y el daño* consiste en la demostración de dependencia entre la conducta de la persona a quien se imputa los hechos y el daño infringido.

Nuestro país es seguidor de la teoría de la responsabilidad civil en materia contractual, así lo manifiesta el autor Edgar Cortes, quien a su vez cita a J. Peirano Facio:

> "Una rápida revisión de la doctrina latinoamericana nos permite ver cómo el criterio de la culpa es punto obligado de partida para el estudio de la cuestión, habida cuenta de las normas codificadas, de la influencia de la bibliografía europea y de la base romanista, como elemento imprescindible para la comprensión e interpretación del sistema. Así un repaso de la doctrina permite corroborar tal afirmación, pues tal es el concepto clásico del fundamento de la responsabilidad civil, fundamento exclusivamente subjetivo que radica en la noción de culpa. Este concepto fue adoptado, prácticamente, por la unanimidad de los códigos civiles redactados hasta épocas recientes. Así ocurre por ejemplo, con los países que más fielmente han recogido las ideas de Andres Bello (arts.1547 y 2329, c.c.chileno;arts.1604,2341 y 2346 c.c.colombiano;arts.1590,3342(sic) y 2256 c.c.ecuatoriano);…"[71]

[70] Arturo Alessandri, *Obligaciones*, s.f., p.194.

[71] Edgar Cortes, *La culpa contractual en el sistema jurídico latinoamericano*, Bogotá, Editorial Salamanca, 2001, p.189.

Frente a la tradicional responsabilidad civil que exige como requisito para que surja la obligación de indemnizar la culpa o negligencia del autor, hoy día avanzan las tesis que defienden la *responsabilidad objetiva o responsabilidad por riesgo*, en que basta que concurran los demás requisitos (acción, nexo causal y daño) sin necesidad de imputar una actuación dolosa al culpable. Se pretende de esta manera proteger a los perjudicados por aquellas actividades que implican cierto riesgo aunque su autor no haya incurrido en culpa.[72]

Así tenemos que para la determinación de la responsabilidad objetiva no se necesita la existencia de los supuestos necesarios para la configuración de la responsabilidad subjetiva de manera particular la existencia de la culpa, siendo necesaria solo la existencia del daño y de una conducta que sirva de fundamento para la imputación de ese daño.

Los partidarios en la aplicación de la teoría de la responsabilidad objetiva, como Ramón Daniel Pizarro, establecen como motivos para que su vigencia: el avance y la diversidad de las actividades económicas y su complejidad; la desigualdad entre proveedores y consumidores; el desarrollo industrial que acarrea la complejidad de las maquinarias y la dificultad de una persona para probar técnicamente el daño que le han causado ésta, de ser el caso.

El autor citado en el párrafo anterior manifiesta:

> "El derecho mira ahora a la víctima más que al victimario, aunque sin desentenderse, por cierto, de la situación de éste. Frente a un daño causado inculpablemente, en virtud de una actividad realizada por la utilización de una cosa que generó un riesgo, es legítimo preguntar: ¿Resulta justo que la víctima quede abandonada a su suerte, sin derecho a reclamar reparación alguna, por el mero hecho de no mediar culpa en la conducta del responsable?. Ante la presencia de dos conductas inocentes, al menos desde el punto de vista subjetivo – la víctima y el autor del daño (o el responsable del mismo) – las modernas corrientes de nuestro tiempo

[72] Enciclopedia Jurídica. *Responsabilidad Objetiva.* http://www.enciclopedia juridica.biz14.com/d/responsabilidad-objetiva/responsabilidad-objetiva.htm. s.f.

se inclinan por la primera, por ser ella quien sufrió el perjuicio y en razón de la necesidad de restablecer el equilibrio alterado por el hecho dañoso"[73]

Se infiere que fueron los avances industriales y tecnológicos los que modificaron la forma de interpretar la responsabilidad jurídica por los daños, excluyendo la culpa como un elemento esencial de la responsabilidad, ya que se considera que ésta " es una noción poco precisa, poco científica que adolecía de los elementos que debe contener un término jurídico, lo que impedía la realización de una organización realmente técnica de la responsabilidad civil; además se atacaba por la dificultad que generaba su prueba, se desahuciaba a la víctima con la consideración de no haber logrado suministrar la prueba de la conducta del autor del daño y era aquélla en último término la que debía soportar pasivamente la ruptura de los derechos, sin posibilidad alguna de obtener reparación cabal del perjuicio". [74]

La responsabilidad objetiva se fundamenta en el resultado o actividad, protegiendo dentro del ámbito de esta última a toda actividad que genere un riesgo y que sea susceptible de ocasionar un daño. Este tipo de responsabilidad se basa en la *teoría del riesgo creado*, que busca elevar el daño a la categoría de elemento estructural de la responsabilidad. Esta doctrina, según el autor colombiano Pizarro, puede ser sintetizada de esta manera: "quien se sirve de cosas que por su naturaleza o modo de empleo generan riesgos potenciales a terceros, deben responder por los daños que ellas originan; quien realiza esta actividad debe cargar con los resultados dañosos que ella genere a terceros, sin prestar atención a la existencia o no de una culpa del responsable."[75]

Con relación al tema que nos ocupa debemos preguntarnos si el uso del internet o la utilización de los servicios bancarios constituyen actividades riesgosas que permitan aplicar la teoría en mención.

---

[73] Ramón Daniel Pizarro, *Responsabilidad Civil por el Riesgo o Civil de las cosas*, p.32.

[74] Jorge Santos Ballesteros, Instituciones de Responsabilidad Civil, citado por Daniel Peña Valenzuela, *Responsabilidad Civil en la Era Digital*, Bogotá, Proyectos Editoriales Curcio Penen, Bogotá, 2007, p.45.

[75] Ramón Daniel Pizarro, *Responsabilidad Civil por el Riesgo o Civil de las cosas*, p.38.

En lo referente al *internet* se debe partir de que el uso del mismo es una actividad interactiva, global y abierta, que supone la actuación no únicamente del individuo frente a un computador, sino de otros sujetos que pueden eventualmente captar y dar un tratamiento específico a los datos de los usuarios de internet lo que se denomina *recogida de datos*, facilitados por ciertos protocolos y rutas de acceso. Esto permite por ejemplo que un proveedor de acceso a internet pueda conocer todos los servidores que ha contactado un usuario o datos de conexión. Así por ejemplo gracias a estas actuaciones se puede establecer si un ordenador está apagado o no, por lo que en el proceso de navegación surgen una infinidad de datos que pueden ser recopilados por los sujetos que intervienen en el proceso de navegación, entre ellos: proveedor de servicios; operador de telecomunicaciones, proveedores de acceso y de servicios a internet, servidores proxy (direcciones IP visitadas); por los enrutadores o routers.[76]

Como vemos el uso del internet si bien es de fácil acceso puede suponer un peligro no necesariamente por lo que el usuario haga sino porque los datos del usuario inevitablemente pueden ser recogidos por terceras personas, por lo que es necesario que este avance tecnológico vaya de la mano de una adecuada información sobre todo de los proveedores de servicios. En lo que respecta a la banca existe un esfuerzo por concientizar a los usuarios por los peligros ocasionados por el uso de los canales electrónicos.

En lo atinente *a la banca*, los detractores de la aplicación de la responsabilidad objetiva a la actividad bancaria afirman que "la empresa bancaria asume un riesgo profesional, ya que en realidad el banco no crea una actividad peligrosa. De modo que, en el supuesto extracontractual responderá de las consecuencias mediatas e inmediatas y necesarias en lo contractual pero no de las remotas, que no tienen nexo adecuado de causalidad con el hecho ilícito." [77]

[76] Daniel Peña Valenzuela, *Responsabilidad Civil en la era digital*, Bogotá, Proyectos Editoriales Curcio Penen, Bogotá, 2007, pp. 51 – 54.

[77] Eduardo Antonio Barbier, *Contratación Bancaria*, p.529.

Mi objetivo principal en la elaboración del presente trabajo es precisar si son suficientes los mecanismos contemplados en la legislación ecuatoriana para establecer la responsabilidad bancaria frente a los delitos informáticos, por lo que es necesario determinar si en el ámbito de estudio, esto es, la responsabilidad civil, nuestra legislación cuenta con las herramientas necesarias para proteger al cliente bancario frente a esta eventualidad.

Para establecer la aplicabilidad de normas civiles en concreto, es necesario considerar varios supuestos.

Como ya he mencionado, la banca ha incursionado a la par de los avances tecnológicos en dos ámbitos: en la banca automatizada y en la banca virtual, en el primer caso involucra a los cajeros automáticos, las tarjetas de crédito y de débito, el dinero digital, los débitos automáticos, la compensación de cheques; mientras que la segunda opción se relaciona al uso del internet para la realización de operaciones bancarias, como por ejemplo las transferencias electrónicas. [78] La utilización de la banca automatizada y de la banca virtual que sin duda ocasiona beneficios tanto para la banca como para el cliente originan un riesgo profesional para la primera, que se traduce en el riesgo operacional del que trate en el capítulo I.

Como todo riesgo profesional el de la banca no puede ser transferido a los usuarios y clientes de esta, ya que al ser la parte fuerte de la relación contractual en sentido económico y jurídico debe asumir el mismo, por tanto es quien debe blindar sus operaciones y actividades contra riesgos delictuales. De ahí que hablamos de la tuición preventiva, empero que ocurre si éstos riesgos llegan a suceder es decir frente a la consumación de un ilícito que bancaria perjudica a los clientes ?

La principal fuente de obligación que une al cliente con el banco es sin duda alguna el contrato bancario que supone la custodia de dinero, es decir que éste adquiere la calidad de depositante. Vale la pena establecer que en materia de protección al cliente a parte del sigilo bancario la protección del ahorro debe tener un tratamiento profesional desde el punto de vista de la tuición y protección al cliente.

[78] Eduardo Antonio Barbier, *Contratación Bancaria*, pp. 17 – 18.

Para Eduardo Barbier "la tutela del ahorrista ha sido justificada por la más conspicua doctrina jurídica, pero sobre todo por las reglas de la economía. Es que al ahorro se debe la existencia misma de la banca, cuya aparición desde tiempos remotos garantizaba la seguridad en el atesoramiento. Sin embargo, para comprender el verdadero interés de la cuestión cabe señalar que el ahorro responde a un impulso natural del hombre para prevenirse de contingencias desfavorables o para concretar sus aspiraciones; de allí que la preocupación por protegerlo trasciende al ámbito puramente economicista para convertirse en una preocupación social"[79]

Pero para el caso que nos ocupa además de la calidad de depositante es necesario que el cliente haya celebrado un contrato de banca en línea o internet. No es de extrañarse que a la par de la suscripción de los contratos de depósito y de cuenta corriente, al cliente se le haga suscribir un contrato de servicios bancarios en línea, en el cual el banco se obliga a poner a disposición del cliente el servicio de banca electrónica por medio de internet o plataformas de transmisión electrónica, sistemas de acceso telefónico a datos y redes privadas virtuales que permiten al cliente utilizar los servicios con la finalidad de consultar el saldo de sus cuentas, realizar operaciones bancarias como transferencia entre cuentas propias o de otras personas, transferencias interbancarias, pagos de impuestos y servicios, realizar solicitudes al banco, renovación de plazos, entre otros, todo lo cual toma el nombre de servicios de banca por internet.

El contrato de servicios de banca en línea conocido en otros países como Argentina como *banca hogareña* es un contrato de prestación de servicios por el cual el Banco dispone de mecanismos técnicos adecuados que le permiten canalizar las órdenes realizadas por el titular de las cuentas es decir por el cliente, por lo que se puede decir que también incluye un mandato.[80] En otros países se conoce a este tipo de contratos como *banca electrónica* o *internet baking* y se lo define como el conjunto de productos y servicios que permiten por medio de los procesos informáticos que el cliente pueda

[79] Eduardo Antonio Barbier, *Contratación Bancaria*, p.127.

[80] Eduardo Antonio Barbier, *Contratación Bancaria*, p.308.

realizar una serie de transacciones bancarias sin necesidad de acudir a la sucursal.[81] En la resolución JB – 2012 – 2148 emitida por la Junta Bancaria del Ecuador, publicada en el Registro Oficial número 727 de 19 de Junio de 2012, se define a la banca electrónica como "los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda."

El contrato de servicio de banca en línea al ser un contrato de adhesión no debe incluir cláusulas abusivas, sobre todo aquellas consistentes en eximir al Banco de responsabilidad por el uso del servicio.

Las *obligaciones* que contrae el Banco para con el cliente exceden de las establecidas en el contrato ya que debe controlar las técnicas y los procedimientos a su cargo para cumplir con éste, por lo que sin ser taxativas las principales son: brindar el servicio mediante la implementación de una adecuada y segura plataforma electrónica que blinde a los usuarios frente a ilícitos cometidos por terceros, cumplir con las órdenes de su cliente. Aquí se debe realizar un paréntesis ya que parecería que lo que he denominado *plataforma electrónica*[82] dependería exclusivamente de la entidad bancaria lo cual es falso ya que el banco debe contratar a su vez sus servicios con otras empresas que son las proveedoras de servicios en internet conocidos como *Service Providers (ISP)* que agrupan a empresas tradicionales de telecomunicaciones y empresas propietarias de portales de internet. Se puede clasificar a estos intermediarios, así las funciones que cumplen: los que permiten a los usuarios el acceso a internet, los que alojan las páginas web en sus servidores, los que permiten el uso de plataformas tecnológicas para servicios en línea, e incluso otros que facilitan herramientas para el pago electrónico. [83]

---

[81] Marianna Fonseca Villanea, *El hecho de un tercero como eximente de la responsabilidad objetiva bancaria* , http://www.ulacit.ac.cr/files/careers/48_fonsecavillanea.pdf.

[82] La resolución JB- 2012 – 2148 no habla de plataforma electrónica sino que utiliza en el numeral 2.41 del Art. 2 el término canales electrónicos y los define como todas las vías o formas de las cuales pueden ser utilizadas por los clientes para realizar transacciones como por ejemplo: dispositivos electrónicos o tecnológicos, como los cajeros automáticos, dispositivos de puntos de venta, señales telefónicas, celulares, e internet.

[83] Daniel Peña Valenzuela, *Responsabilidad Civil en la era digital*, Bogotá, Proyectos Editoriales Curcio Penen, 2007, p.57.

En cuanto a las obligaciones del cliente, las principales son: anticipar los fondos necesarios para efectuar las operaciones bancarias que requiera; satisfacer el pago de comisiones, y sobre todo utilizar procedimientos o medios de seguridad, identificación, integridad y autentificación, entre ellos utilizar un nombre de usuario y contraseña, tarjeta de coordenadas o token (código bisa)[84], claves temporales, preguntas de seguridad, elementos estos que configuran la identificación electrónica, del cliente.

Al respecto de las obligaciones que adquiere el cliente encontramos en nuestra legislación el Art. 8 del Reglamento de la Ley de cheques que establece:

> "**ARTÍCULO 8**.- Los depósitos, retiros de fondos, créditos, débitos y cualquier otra transacción permitida en cuentas de depósitos monetarios, efectuados a través de medios electrónicos o electromecánicos, deberán estar sustentados por un acuerdo escrito entre la institución financiera y el titular de la cuenta, en el que deberán constar, por lo menos, las siguientes condiciones:
>
> **8.1** La responsabilidad del cliente respecto de las transacciones que efectuare a través de estos medios;
>
> **8.2** La responsabilidad del cliente de mantener en secreto la clave o seguridades a él asignadas, así como los cambios de claves que se efectuaren. Igual responsabilidad tendrá con respecto a las claves o seguridades adicionales por él solicitadas y otorgadas por la institución financiera girada; y,
>
> **8.3** La obligación de las entidades financieras de mantener los controles y resguardos que garanticen las seguridades físicas y tecnológicas de este tipo de transacciones, tomando en cuenta los riesgos inherentes a su operatividad."

Se infiere así que la principal obligación de la entidad bancaria es garantizar las seguridades físicas y tecnológicas de las transacciones que realizan los clientes vía

---

[84] La Tarjeta de Coordenadas-Código Bisa es una pieza de plástico del tamaño de una tarjeta de crédito, tiene 80 casillas y cada casilla contiene dos números. Cuando se utiliza este método de seguridad el banco solicita por medio de internet al usuario que ingrese números que están en diversas casillas y que corresponden a la casilla identificada con un número determinado colocado en la parte del costado horizontal y una letra determinada en la parte superior (4G) (5J) (3B) etc.

internet, mientras que la principal obligación del cliente es preservar y asegurar las claves y seguridades por él solicitadas.

En cuanto a los *derechos* que nacen del contrato varios de estos se encuentran establecidos en el Código de Derechos del Usuario del Sistema Financiero, entre los que se encuentran recibir educación financiera y el derecho a la información de productos y servicios financieros, a parte de otros de protección entre los que se encuentran: "Recibir protección de los datos personales que las entidades financieras obtengan del usuario para la prestación de productos y servicios financieros prestados por vía electrónica. Las instituciones financieras adoptarán específicamente las medidas de seguridad necesarias para este tipo de operaciones financieras". [85]

A pesar de los mecanismos de seguridad que debe suministrar el banco y guardar el cliente, éstos son violentados por terceras personas que buscan apropiarse de los depósitos del último, lo que indudablemente coloca en una situación de indefensión a las partes, ya que conforme fue detallado en el capítulo I, entre los mecanismos más usuales está la creación de páginas web falsas y que aparentan ser las de los bancos con la finalidad de obtener información del cliente relacionada con sus cuentas y seguridades para luego utilizarlas y hacer transferencias electrónicas.

El banco se encuentra en la obligación de salvaguardar y asegurar sus plataformas electrónicas en pos de brindar a sus clientes un servicio seguro, pero qué pasa cuando éstas son violentadas?

Nos encontramos ante dos supuestos: 1) Que el Banco sí haya cumplido con todas los protocolos necesarios para evitar tal vulneración y, 2) Que el Banco en efecto haya incumplido con la obligación de brindar un servicio seguro al cliente, es decir no haya previsto de manera adecuada y tecnológica que tal evento dañino suceda. En el primer caso, en el evento que el Banco haya en efecto cumplido con la obligación de brindar al cliente un servicio de banca en línea seguro, esta actuación debe ser

[85] Este derecho de protección consta en el numeral 14.3 del Art. 14 del Código de Derechos del Usuario del Sistema Financiero expedido mediante resolución No JB – 2010 – 1782 de 19 de Agosto del 2010; y, trasladado del título XX al título XIV y reenumerado con resolución Nro. JB – 2013 – 2393 de 22 de Enero del 2013.

complementada con otras obligaciones que en nuestro país le impone tanto la Ley de Defensa del Consumidor como el Código de Derechos del Usuario del Sistema Financiero como son: la de haber suministrado una adecuada educación financiera; la de haber otorgado información de sus productos y servicios financieros; la de dar oportunidad al cliente de elegir sobre los servicios que contrata; la de acceder a la documentación a la información y documentación. Solo si el Banco cumplió con todas las obligaciones que no solo le fueron impuestas en el contrato sino las que a normativa legal exige se podría decir que existe un evento insuperable lo que le exoneraría de responsabilidad.

Asimilando el tema en análisis a la responsabilidad bancaria ante los robos de cajas de seguridad; "La cuestión se centra en torno al nivel de la diligencia exigible a la entidad de crédito, y, más en torno a si el robo es un suceso que entra en la esfera del riesgo de la actividad bancaria…hoy en día el debate encuentra su máxima expresión en si el robo con empleo de la tecnología más moderna merece o no el calificativo de insuperable lo que exoneraría al banco de toda responsabilidad…el robo se ha desarrollado con tal magnitud de adelantos técnicos y científicos que hace imposible en todo caso, que la entidad de crédito hubiera podido evitarlo por más esfuerzo que hubiera puesto en el empeño."[86]

Como vemos es discutible la responsabilidad bancaria frente al delito informático ya que bien pudo la entidad haber cumplido todas las exigencias contractuales y legales. En mi opinión, a pesar de que el banco representa la parte fuerte de la relación contractual frente al cliente, su responsabilidad no debe ser determinada en consideración única y exclusivamente a este criterio sino que debe ser establecida en un proceso judicial en el que se le dé la oportunidad al menos de manifestar su posición, en pos de garantizar el debido proceso y el derecho de legítima defensa.

Pero ¿qué ocurre si el Banco incumplió con la obligación de brindar canales electrónicos y plataformas tecnológicas adecuadas y seguras para evitar el cometimiento

[86] Julio Alvarez Rubio, *Derecho de Obligaciones*, Obra Jurídica Enciclopédica, México, Editorial Porrúa, 2012, pp. 224 – 225.

de delitos informáticos contra sus clientes?. Para la determinación de la responsabilidad que asumiría el banco, en el evento que exista una reclamación judicial del cliente, el juzgador deberá realizar un análisis jurídico partiendo del estudio de las obligaciones que contrajo la entidad bancaria. *En virtud de lo expuesto, bien vale la pena preguntarse ¿qué clase de obligación contrae el Banco para con el cliente de conformidad con nuestras normas civiles en referencia al contrato de banca electrónica?*.

Para ello es necesario recordar la clásica división de las obligaciones en DAR; HACER; y, NO HACER.

La clasificación mencionada es de extrema importancia al momento que en la praxis se la debe tomar en cuenta para entablar una acción, pues cada una de estas categorías delimita lo que podemos plantear en relación a los perjuicios; así si la obligación es de dar aplicaremos el Art. 1564 del Código Civil[87], si la obligación es de hacer aplicaremos el Art. 1569[88] del mismo cuerpo legal y, si la obligación es de no hacer tendremos que aplicar el Art. 1571 del citado Código. [89]

Las *obligaciones de hacer*, son consideradas obligaciones positivas, se encuentran constituidas por una prestación, acción, comportamiento, conducta , que justamente consisten es un hacer, producir, realizar y, o ejecutar algo. Según la autora Virginia Pardo Iranzo, las obligaciones de hacer "son aquellas cuya prestación consiste en la realización de una actividad diferente de la de entregar una cosa. Se definen por tanto de manera negativa ya que entregar una cosa también es un

[87] "Art. 1564. Obligación de dar.- La obligación de dar contiene la de entregar la cosa; y si ésta es una especie o cuerpo cierto , contiene, además la de conservarlo hasta la entrega, so pena de pagar los perjuicios al acreedor que no se ha constituido en mora de recibir".

[88] "Art. 1569.- Si la obligación es de hacer, y el deudor se constituye en mora, podrá pedir al acreedor, junto con la indemnización de la mora, cualquiera de estas dos cosas a elección suya: 1. Que se le autorice para hacerla ejecutar por un tercero, a expensas del deudor; y, 2. Que el deudor le indemnice los perjuicios resultantes de la infracción del contrato".

[89] "Art. 1571.- Toda obligación de no hacer una cosa se resuelve en la de indemnizar los perjuicios, si el deudor contraviene y no puede deshacerse lo hecho. Pudiendo destruirse la cosa hecha, y siendo su destrucción necesaria para el objeto que se tuvo en mira al celebrar el contrato, estará el deudor obligado a ella, o autorizando al deudor para que la lleve a ejecución a expensas del deudor. Si dicho objeto puede obtenerse cumplidamente por otros medios, será oído el deudor que se allane a prestarlos. El acreedor quedará de todos modos indemne".

hacer…Las obligaciones de facere tienen siempre un objeto indeterminado (incertum); aunque el resultado de la operación (p.ej. la casa ya construida) esté previsto como concreto, el hacer mismo es previamente indeterminado."[90]

Por otra parte la autora citada manifiesta que las obligaciones de hacer pueden ser de medio y resultado, clasificación que es importante a efectos de determinar lo que el acreedor puede exigir como contenido de su derecho de crédito. En las obligaciones de medio (también llamadas de mera actividad o de diligencia) el deudor se compromete a mantener una determinada actitud (una actividad diligente), mientras que las obligaciones de resultado la prestación consiste en alcanzar una determinada meta; el objeto de la obligación no es, simplemente, mantener una determinada actitud, sino conseguir un determinado resultado.[91]

La obligación del banco frente al cliente en el tema que nos ocupa es de hacer y desde mi punto de vista, una obligación de resultados, afirmación que se origina, como se ha mencionado hasta el momento, en la tecnificación con la que debe contar una entidad bancaria para brindar un servicio seguro y óptimo dado su alto grado de profesionalización de ésta actividad que supone llevar a cabo todo un proceso no solo de custodia de los dineros de los depositantes sino de preservación de los mismos, tanto más cuanto que, al momento de hacerle firmar al cliente un contrato de banca en línea o bien si el cliente solicita éste, el Banco se obliga a brindar e implementar medios tecnológicos.

Para entender esta parte veamos como se redacta la oferta del servicio por parte del Banco en un contrato de esta naturaleza:

> "El BANCO, con el fin de proporcionar servicio a través de canales tecnológicos a sus clientes cuenta entre otros con sistemas de cajero automático; phonored; portal electrónico, terminales de autoconsulta, una estructura completa de servicios vía Centro de Llamadas telefónicas (Call

[90] Virginia Pardo Iranzo, Ejecución de Sentencias por obligaciones de hacer y de no hacer, Valencia, Tirant lo Blanch; 2001, pp. 143 – 144.

[91] Virginia Pardo Iranzo, *Ejecución de Sentencias por obligaciones de hacer y de no hacer*, pp. 146 – 149.

> Center), *sin limitar los servicios que se implementen a futuro,* servicios a los que se puede acceder a través de cajeros automáticos, de aparatos telefónicos, del Internet, de terminales electrónicas computarizadas o de cualquier otro medio electrónico o telemático *que se implemente a futuro*."[92]

De la cláusula transcrita tenemos que el Banco utiliza para referirse a los servicios que brinda el verbo *implementar*, que supone una actividad. *Implementar* significa poner en funcionamiento, aplicar métodos, medidas, etc., para llevar algo a cabo. En el transcurso de un proceso judicial será importante la comprobación de que en efecto el Banco cumplió con la obligación asumida para efectos de determinar su culpa o no.

La obligación de hacer que el Banco contrae en el momento de la firma del contrato de banca en línea, presupone que éste ya cuenta con este servicio es decir con la plataforma electrónica previamente implementada que es puesta a disposición del cliente, y por ello no se podría manifestar que a su vez a parte de una obligación de hacer, la contraída por el Banco es una obligación a plazo, entendido éste según nuestro Código Civil en su Art. 1510 como "la época que se fija para el cumplimiento de la obligación", ya que la prestación es cumplida por el Banco de manera inmediata a la suscripción del contrato en el momento en el que el cliente accede al servicio de banca en línea.

La obligación del banco se torna así en una obligación de tracto sucesivo, es decir una obligación que no es realizada en un solo acto, sino que debe ser reiterada durante un tiempo determinado, debiendo garantizar la entidad bancaria no solo el comienzo de la realización de la actividad, sino también su realización continuada.[93]

Sin embargo si esa obligación de hacer contraída por el Banco se cumplió, pero de manera imperfecta, nos encontramos ante el derecho del cliente de reclamar la indemnización de daños y perjuicios proveniente del incumplimiento del contrato de

[92] La cláusula transcrita consta en un contrato de banca en línea celebrado entre una entidad bancaria y una persona natural.

[93] Virginia Pardo Iranzo, *Ejecución de Sentencias por obligaciones de hacer y de no hacer*, p.21.

banca en línea conforme lo preceptúa el Art. 1572 del Código Civil que establece: "La indemnización de perjuicios comprende el daño emergente y el lucro cesante, ya provenga de no haberse cumplido la obligación, o de haberse cumplido imperfectamente, o de haberse retardado el cumplimiento". La norma transcrita presupone dos hechos: que una de las partes no cumplió con su obligación o que cumplida lo hizo de manera imperfecta.

Como lo habíamos mencionado anteriormente, para establecer la responsabilidad civil en la esfera bancaria desde el punto de vista de la responsabilidad subjetiva deben confluir tres elementos: la existencia del factor culpa; la imputabilidad de ésta a una persona determinada; la existencia del daño o perjuicio; y, el nexo causal entre la culpa y el daño.

Hace más de quince años, cuando la banca empezaba a incursionar en los servicios de banca en línea se estableció que para establecer la responsabilidad por transferencias no autorizadas se debía determinar la culpa tanto del cliente como la de los bancos, al respecto se manifestó:

> " Se impone por tanto, una solución intermedia que en nuestro ordenamiento, y en general, se basa en la culpa y la limitación de los daños resarcibles…La responsabilidad por culpa tiene el gran mérito de imponer un deber de diligencia en relación con los dos principales sujetos de un sistema electrónico de fondos: el cliente y el banco. No existen dudas acerca de que la mejor garantía contra la realización de transferencias no autorizadas de fondos es el comportamiento diligente del cliente, y en particular en lo que atañe al extravío y hurto de su tarjeta de crédito y de su número de identificación personal"[94]

Para determinar la especie de culpa por la que responde el banco por haber incumplido de manera imperfecta con su obligación debemos recordar las especies de culpa determinadas en el Art. 29 del Código Civil:

[94] Gianantonio Ettore, *Informática y Derecho*, Volumen 3, Transferencia Electrónica de Fondos y Autonomía Privada, (Coordinadores: Ricardo Altmack y Rafael Bielsa), Buenos Aires, Ediciones Depalma, 1997, p.31.

> “La ley distingue tres especies de culpa o descuido. Culpa grave, negligencia grave, culpa lata es la que consiste en no manejar los negocios ajenos con aquel cuidado que aún las personas negligentes y de poca prudencia suelen emplear en sus negocios propios. Esta culpa, en materias civiles, equivale al dolo.
>
> *Culpa leve, descuido leve, descuido ligero, es la falta de aquella diligencia y cuidado que los hombres emplean ordinariamente en sus negocios propios. Culpa o descuido, sin otra calificación, significa culpa o descuido leve. Esta especie de culpa se opone a la diligencia o cuidado ordinario o mediano. El que debe administrar un negocio como un buen padre de familia es responsable de esta especie de culpa*.
>
> Culpa o descuido levísimo, es la falta de aquella esmerada diligencia que un hombre juicioso emplea en la administración de sus negocios importantes. Esta especie de culpa se opone a la suma diligencia o cuidado. El dolo consiste en la intención positiva de irrogar injuria a la persona o propiedad de otro. ”

La norma transcrita debe ser analizada en concordancia con lo dispuesto en el Art. 1563 del Código Civil:

> “Art. 1563.- El deudor no es responsable sino de la culpa lata *en los contratos* que por su naturaleza, sólo son útiles para el acreedor; *es responsable de la leve es responsable que se hace para beneficio recíproco de las partes*; y de la levísima, en los contratos que el deudor es el único que reporta beneficio.
>
> El deudor no es responsable del caso fortuito, a menos que se haya constituido en mora, siendo el caso fortuito de los que no hubieran dañado a la cosa debida, si hubiese sido entregada al acreedor, o que el caso fortuito haya sobrevenido por su culpa.

*La prueba de la diligencia o cuidado incumbe al que ha debido emplearlo; y la prueba del caso fortuito al que lo alega***.**

Todo lo cual se entiende sin perjuicio de las disposiciones especiales de las leyes, y de las estipulaciones expresas de las partes."

Estas disposiciones nos ayudan a dilucidar qué especie de culpa incurre el banco y a cuál de las partes incumbe probar ésta, partiendo del beneficio que reporta a las partes el contrato de banca en línea.

Por las características que hasta el momento tenemos del contrato de banca en línea y siguiendo las definiciones de las distintas clases de contratos según la clasificación que va del Art. 1455 al 1459 del Código Civil, diremos que el contrato de banca en línea es un contrato: *oneroso* ya que tiene por objeto la utilidad de ambos contratantes, es decir en beneficio mutuo; *no conmutativo* debido a que las prestaciones contraídas entre el Banco y el cliente no son equivalentes[95]***;*** *accesorio* al contrato de depósito de ahorros o cuenta corriente (para el caso del cliente bancario contractual); y, *consensual* como consecuencia de que se perfecciona con el solo consentimiento de las partes, que en este sentido debe ser un consentimiento que conste por escrito ya que se debe predeterminar las obligaciones del Banco y del cliente pero además considerando el beneficio que se da tanto para el uno como para el otro debido a que el Banco por el servicio que brinda se beneficia económicamente puesto que las transferencias bancarias vía internet tienen una tarifa mientras que el cliente se beneficia del uso del servicio, circunstancias éstas fundamentales para establecer que, de conformidad con el primer inciso del Art. 1563 del Código Civil tenemos que el contrato de banca en línea al ser un contrato en beneficio tanto del cliente como del banco supone que en el caso de incumplimiento de las obligaciones de éste último incurriría en *culpa leve***.**[96]

[95] Teniendo en cuenta que el contrato conmutativo es aquel en que genera obligaciones equivalentes y recíprocas entre las partes, desde mi punto de vista si bien el contrato de banca en línea genera obligaciones reciprocas estas no pueden tenerse como equivalentes ya que frente al alto grado de tecnificación y profesionalización de la entidad bancaria el cliente asume una contraprestación únicamente de pago del servicio, lo que evidentemente hace que entre una y otra prestación no exista equivalencia.

[96] Se dirá que los bancos por la incidencia de su servicio deben contar con un alto grado de tecnificación, eso es indudable, por lo que debe emplear en sus actuaciones una esmerada diligencia lo que implicaría

Para corroborar lo manifestado cito Arturo Alessandri, quien manifiesta:

> "..si el contrato beneficia únicamente al acreedor, el deudor responde sólo de culpa grave: acontece en el contrato de depósito que va únicamente en beneficio del acreedor….Cuando el contrato va en utilidad del acreedor y del deudor, el deudor responde de culpa leve, como en el contrato de arrendamiento…Se responde de culpa levísima en los contratos que están establecidos e beneficio exclusivo del deudor. Ello es natural. Acontece de esta manera en el contrato de comodato…Así todo esto parece útil. Pero en la práctica la cuestión se dificulta porque en definitiva quedará a la apreciación del juez determinar si un acto del deudor constituye una u otra culpa. Y puede acontecer que mientras un juez califique una culpa de grave, otro la califique de leve."[97]

Sobre la base de esta conclusión cabe preguntarse, si ante el cometimiento de un delito informático de apropiación ilícita es posible que el cliente pruebe dentro de un proceso judicial que las plataformas tecnológicas fueron efectivamente vulneradas, *no existiendo la reversión de la carga de la prueba en materia civil*.[98]

La respuesta nos la da el propio Art. 1563 en su inciso tercero al establecer: *"La prueba de la diligencia o cuidado incumbe al que ha debido emplearlo; y la prueba del*

---

que la falta de ésta nos colocaría frente a una culpa levísima, empero para determinación de responsabilidades contractuales es la propia ley la que determina la especie de culpa atendiendo al beneficio que reciben las partes. Es decir que ante otros eventos por ejemplo la determinación de una quiebra culposa hablaríamos de culpa levísima en atención a lo manifestado.

[97] Arturo Alessandri, *Obligaciones*, s.f. , p.197.

[98] Según el Código de Procedimiento Civil Ecuatoriano en su Art. 113 establece la responsabilidad procesal de la prueba disponiendo por regla general la carga de la prueba corresponde al actor. Sin embargo en otras normas de otros cuerpos legales se dispone una inversión de la carga de la prueba de ciertos hechos y actos al demandado, así por ejemplo en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional se establece en el último inciso del Art. 16 que cuando la entidad pública accionada no demuestre lo contrario o no suministre la información solicitada se presumirán ciertos los hechos de la demanda. Por la época en que fue redactado nuestro Código Civil no hablaría la autora propiamente de una "inversión de la carga probatoria"

*caso fortuito al que lo alega***."** Es importante recalcar que en materia de consumo también existe la inversión de la carga de la prueba ya que:

> "En el Derecho del Consumidor, quien debe probar que no es culpable es el proveedor. A él le corresponde presentar todos los presupuestos fácticos, técnicos, económicos para demostrar su inocencia. El consumidor, por su limitación para contar con las pruebas, no está obligado a probar los fundamentos de su reclamo o acusación." [99]

La disposición y principio arriba enunciados se basan en el hecho que la culpa en materia contractual no debe ser probada por quien la alega, sino que el deudor, en este caso el banco, es quien debe acreditar que ha empleado la diligencia debida. [100]

Aunque se ha manifestado que la vulneración de las plataformas informáticas de un banco es de difícil comprobación, la determinación de la culpa de la entidad bancaria frente a un delito informático se basa en el simple hecho de que los sistemas del banco en un caso concreto fueron efectivamente vulnerados ya que *el que debe demostrar que empleo la diligencia y cuidado es el Banco*, lo que si bien no constituye reversión de la prueba constituye una disposición que en cierto modo favorece al cliente bancario, ya que en los respectivos procesos judiciales será el Banco el que tenga la obligación jurídica de demostrar por intermedio de los respectivos medios probatorios establecidos en nuestra legislación que en efecto en la ejecución del contrato de banca en línea empleó la *diligencia* y *cuidado* debidos, entendidos éstos como sinónimos ya que una de las acepciones de diligencia es cuidado en ejecutar algo, mientras que cuidado es la diligencia o la debida atención que debemos poner en *hacer* una cosa.

Queda así demostrado que en nuestra legislación civil sí existe la normativa adecuada para proteger al cliente bancario frente a las consecuencias civiles del delito informático ya que el riesgo no puede ni debe ser transferido a los clientes.

---

[99] Haydeé Alvarado, *Derecho del Consumidor*, primera parte, texto guía, Loja, Editorial de la Universidad Técnica Particular de Loja, 2006, p.24.

[100] Arturo Alessandri, *Obligaciones*, s.f., p.197.

Como lo analizaré en la parte final de este trabajo, en el año 2011 en nuestro país se suscitó un hecho inédito al expedirse por parte de la Fiscalía General del Estado y de la Superintendencia de Bancos y Seguros dos resoluciones mediante las que se estableció *la responsabilidad civil objetiva* de los bancos ante sus clientes víctimas de delitos informáticos, sin dar a las entidades bancarias el más mínimo derecho a la defensa que debe existir en un proceso de cualquier naturaleza frente a dos posiciones contradictorias. Como se ha analizado, el contrato de servicio de banca electrónica impone obligaciones tanto para la entidad bancaria como para el cliente, cuyo cumplimiento para cada caso solo puede ser discutido dentro de un proceso cualquiera sea el nombre que adopte, más aún si en nuestro país al momento en que se expidieron las mentadas resoluciones sí existían normas de las que podían hacer uso las personas para hacer valer sus derechos ante la banca.

Como se puede apreciar he tratado de enmarcar la responsabilidad de los bancos frente al delito informático de apropiación ilícita de fondos de sus clientes en la esfera civil, sin embargo no debemos dejar de mencionar importantes normas que protegen al cliente en un eventual proceso judicial como son aquellas contempladas en la Ley Orgánica de Defensa del Consumidor, de manera particular las contemplada en los Arts. 28 y 31, normas que establecen que frente a violaciones de dicha ley, las indemnizaciones que perciben los perjudicados son de naturaleza civil, existiendo además una cadena de solidaridad no sólo de quien ofrece el servicio sino en todo aquel que haya influido en dicho daño lo que incluye los proveedores de los servicios electrónicos que contratan los bancos, en el caso que nos ocupa.

Los proveedores en mención son los obligados a suministrar al usuario o consumidor la información para el correcto uso de los servicios electrónicos de conformidad con lo establecido en el Art. 50 de la Ley de Comercio Electrónico.[101]

[101] La disposición en mención establece: "En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento. Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados. La publicidad, promoción e información de servicios electrónicos, por

Hago alusión a la norma mencionada para establecer que la insuficiente o exigua información que el Banco entrega al cliente relativa al buen manejo de los servicios electrónicos por medio de internet y que fue contratado al suscribir el contrato de banca en línea por éste, es también imputable al prestador del servicio de internet, que resulta civil y solidariamente responsable del al ilícito analizado frente al cliente conforme lo preceptúa el Art. 28 de la Ley Orgánica de Defensa del Consumidor.[102]

La responsabilidad de los prestadores de servicio de internet podría ser incluso considerada como eximente de la responsabilidad de la entidad bancaria ya que se ha establecido que "tanto el banco como el cliente, son ambos usuarios de la plataforma de comunicación denominada internet, la cual es de acceso público. El Banco no le ofrece a su cuentahabiente el servicio de internet, sino que le da al cliente la opción de accesar a sus cuentas, recurriendo para ese fin, a la plataforma de uso público, tal cual autopista de información."[103]

Al respecto existen opiniones que consideran que en el caso de los prestadores de servicios de internet tienen responsabilidad objetiva: "Bajo el análisis planteado, teniendo en cuenta los argumentos y elementos encontrados, se puede concluir que la responsabilidad de las empresas que brindan servicio de búsqueda de información por internet es objetiva. Ello en tanto se ha dicho que son las empresas quienes lo ofrecen el servicio, devolviendo información, incluso generando una especie de atención en ciertas páginas, a través de un ranking – pagerank-. Son estas empresas quienes desarrollan el

---

redes electrónicas de información, incluida la Internet, se realizará de conformidad con la ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.
En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o servicio de que se trate.

[102] "Art. 28.- Serán solidariamente responsables por las indemnizaciones civiles derivadas de los daños ocasionados por vicio o defecto de los bienes o servicios prestados, los productores, fabricantes, importadores, distribuidores, comerciantes, quien haya puesto su marca en la cosa o servicio y, en general, todos aquellos cuya participación haya influido en dicho daño".

[103] Marianna Fonseca Villanea, "*El hecho de un tercero como eximente de responsabilidad objetiva bancaria*, Rhombus Derecho, No 01 2009, 10 http://www.ulacit.ac.cr/files/careers/48_fonsecavillanea.pdf. Revisado el 10 de Noviembre del 2014.

diseño del sistema, poseen el software e infraestructura necesaria que les permite colocar el producto en el mercado, y obtener beneficios por dicha actividad" [104]

Como se puede advertir existen distintas posiciones, pero más allá de éstas se debe reflexionar sobre el derecho de las partes intervinientes en un contrato a solucionar sus divergencias y controversias sin que se pueda violentar el derecho de una de ellas a defenderse.

2.3.- RESPONSABILIDAD PENAL DE LA BANCA.-

La responsabilidad penal se distingue de la responsabilidad civil en cuanto en la primera se está a las consecuencias jurídicas predeterminadas por una ley, que el ordenamiento jurídico señala como consecuencia de la realización de un acto comisivo u omisivo doloso que reviste los caracteres de punible, mientras que la civil consiste en imputar a una persona una obligación reparativa en razón del daño que ha causado a otra persona por una conducta culposa de quien causo el daño.[105]

Los bancos para su funcionamiento deben asumir formas societarias. En nuestro país por expresa disposición legal, los bancos privados deben ser sociedades anónimas.[106] Las sociedades anónimas son personas jurídicas que hasta antes de la expedición del Código Integral Penal no podían ser sujetos activos del delito, salvo casos específicamente establecidos en la ley, como es el de quiebra fraudulenta.

Los principales obstáculos para la determinación de la responsabilidad penal de la persona jurídica antes de la expedición del COIP, tenían que ver con tres

---

[104] José María Lescano, *Análisis de la Responsabilidad Civil de los buscadores de Internet*, Anales, Universidad Nacional de la Plata, http://sedici.unlp.edu.ar/bitstream/handle/10915/21019/Documento_completo.pdf?sequence=1. Revisado en Septiembre del 2014.

[105] Gladys Santana – Helem Sánchez y otro. *Cuadro comparativo de la responsabilidad civil y penal*, Universidad La Gran Colombia, Facultad de Derecho, Bogotá – Mayo – 2013, http://es.slideshare.net/helemaleja/cuadro-comparativo-rcc-vs-rce-rc-vs-rp. Revisado en Septiembre del 2014.

[106] Art. 389 del Código Orgánico Monetario y Financiero: "Las entidades del sector financiero privado se constituirán ante la Superintendencia de Bancos como sociedades anónimas, de conformidad con el presente Código, con un mínimo de dos promotores. Se podrá constituir una entidad financiera privada por iniciativa de los promotores interesados, fundadores o por promoción pública".

imposibilidades : a) la imposibilidad de imputar a ésta una acción u omisión, ya que se ponía en entredicho que la persona jurídica pueda actuar independientemente de la voluntad de sus socios; b) la imposibilidad de *culpabilizar* a una persona jurídica de un acto; y, c) la de imposibilidad de que cumpla una pena.

Los obstáculos mencionados parten ante todo del análisis de lo que significa la "acción" y la "voluntad" desde el punto de vista penal, y la imposibilidad de que al ser la persona jurídica un ente ficticio pueda actuar independientemente de la voluntad de sus socios, ya que se concluye, para autores como Jiménez de Asua, que el único que puede actuar con voluntad es el hombre. Dicho autor manifiesta:

> "Cuando estudiemos los elementos intelectuales del dolo se verá que ellos son el conocimiento de los hechos y de su significación. Estos elementos intelectuales se reputan por muchos penalistas como problema general de la culpabilidad. Sea así, o, como nosotros creemos, tan solo contenido del dolo, es lo cierto que sin tal conocimiento fáctico o antijurídico, la culpabilidad no puede edificarse; al menos no puede construirse en su más distintiva especie. Las personas morales no son capaces del conocimiento de los hechos y de su significación injusta, y en consecuencia no pueden ser culpables. Si la culpabilidad es una de las características básicas de la infracción penal, es obvio que las sociedades no pueden perpetrar delitos."[107]

Empero el punto de vista de la inimputabilidad penal de la persona jurídica ha sido dejado de lado desde hace ya algunos años, de manera particular en Europa, por lo que conviene conocer cual es el fundamento jurídico que permite hoy por hoy tal imputación.

Zugaldia Espinar citado por la Dra. Paulina Araujo Granda señala en síntesis: a) En primer lugar las personas jurídicas al igual que las personas naturales sí son susceptibles de someterse al principio de acción, en cuanto son destinatarias de normas

[107] Luis Jiménez de Asua, *Principios del Derecho Penal*, La ley y el delito, 4ta edición, Buenos Aires, Editorial Sudamericana, 2005, p. 211.

jurídicas y capaces de ocasionar los efectos jurídicos contenidos en la misma norma, pueden celebrar contratos por ejemplo que serán perceptibles en la sociedad por intermedio de sus representantes, y b) Se habla por otra parte de lo que se denomina "defecto de organización" como principio sobre el que se basa la doctrina de la responsabilidad penal de la persona jurídica, que a su vez se origina en el aumento del riesgo de la actividad empresarial.[108]

En el Ecuador antes de la expedición del COIP no eran las personas jurídicas las que respondían sino sus directivos o representantes legales en casos específicos cometidos por ellos como en el caso del peculado bancario, quiebras, lavado de dinero.[109]

Al igual que para el análisis de la responsabilidad civil debemos tener partir de la suposición que frente al delito informático, la banca y el cliente de ésta son víctimas del delito, ya que en la gran mayoría de casos son personas extrañas al sistema bancario quienes vulneran las seguridades de éste a fin de provocar una acción dañosa. Ahora bien, también debemos partir de otro presupuesto cual es que una sola institución bancaria se vea afectada por una numerosa cantidad de delitos informáticos que afecten a sus clientes. En el ámbito penal, aquella institución se vería en la obligación de denunciar tal ilícito ante las autoridades para activar la justicia penal, aunque sabemos que tal posibilidad sería poco operable por cuanto sería el propio banco el que ponga al descubierto los sistemas informáticos que posee para atención a su clientes. Por tanto, debo concluir que la responsabilidad bancaria frente al delito informático que afecta a sus clientes no existe no solo por no estar tipificado como delito sino porque como de manera reiterada he manifestado, la entidad bancaria también es víctima del delito informático.

Sin embargo del criterio esgrimido existen autores nacionales como el Doctor Santiago Acurio del Pino y extranjeros tal es el caso de Alberto Sanchez Súarez quienes

[108] Paulina Araujo Granda, *La Nueva Teoría del delito Económico y Empresarial en el Ecuador*, pp. 77 - 78.

[109] Delitos que en el extinto estaban tipificados como se indica: Peculado Bancario (Art. 257 – A.); Quiebra (Art. 576); estafa (Art. 563). En cuanto al lavado de Activos esta contemplada en la Ley para reprimir este delito, en el Art. 14.

defienden la idea de que los representantes legales de los bancos frente al delito informático que afecta a sus clientes son autores del delito de comisión por omisión ya que manifiestan que el banco, por intermedio de sus personeros, al no cumplir con las obligaciones propias del contrato de banca en línea como es la de brindar al cliente una adecuada plataforma tecnológica, está incurriendo en una omisión, configurándose así una violación al deber objetivo del cuidado y con ello el cometimiento de un delito.

El autor nacional Santiago Acurio del Pino, recoge el criterio mencionado fundamentándose en el del autor Alberto Sanchez Súarez que en su libro: "La Estafa Informática", establece al respecto:

> "La creación del riesgo de la producción de la transferencia no consentida procede de una conducta realizada por quien omitió la acción de haberse impedido tal resultado nocivo pues el garante se limitó a no evitar la continuación del curso causal que se originó fuera de su competencia. El sujeto obligado a evitar la producción del resultado nocivo no cumplió con una posición de garante y además hay una equivalencia valorativa entre la omisión realizada y la conducta típica del delito analizado. A pesar que el sujeto no creó el riesgo de producción de esa transferencia de activos perjudicial para el bien jurídico si lo incremento pues no hay duda que si hubiera tomado la acción debida el resultado nocivo no se hubiera ocasionado. El contenido del injusto de quien no realizo la acción para evitar la producción del resultado lesivo para el patrimonio es equivalente a la de quien realiza la manipulación informática que determina la transferencia patrimonial que a su turno causa perjuicio, es decir aquel tiene la misma relevancia que éste porque se presenta como causa determinante de la producción del resultado típico."[110]

No comparto esta opinión ya que he analizado hasta el momento que el banco al igual que el cliente son víctimas de un ilícito cometido por un tercero, no siendo así el primero autor de ningún delito sino tan solo responsable civilmente en determinados

[110] Santiago Acurio del Pino, *Fundamentos de la Responsabilidad de las Instituciones Financieras frente al Delito de Fraude Informático* (Apropiación Ilícita), Universidad Andina Simón Bolívar, 2012, p.16.

casos. Pero como lo hemos analizado, al establecer como sujeto activo de la infracción a la persona jurídica en el COIP enfrentamos una realidad, de la que no pueden sustraerse los bancos por ser personas jurídicas de derecho privado. El COIP establece los siguientes presupuestos para que una persona jurídica sea penalmente responsable, establece el Art. 49 del mencionado cuerpo legal, en síntesis:

1.- Son sujetos del delito la persona jurídica, nacional o extranjera, como tal por la acción u omisión de quienes ejercen la propiedad de ésta o control, sus órganos de gobierno o administración, apoderados (as), mandatarios (as), representantes legales o convencionales, agentes , operadoras u operadores, factores, delegadas o delegados, terceros que contractualmente o no se inmiscuyan en una actividad de gestión, ejecutivos principales o quienes cumplan actividades de administración, dirección y supervisión y, en general, por quienes actúen bajo órdenes o instrucciones de las personas naturales citadas.

2.- La persona jurídica sea regulada por normas de Derecho Privado, lo cual excluye a las personas jurídicas de Derecho Público.

3.-El delito que se cometa debe ser uno de los tipificados en el Código Orgánico Integral penal.

4.- El delito cometido debe tener la finalidad de generar beneficio propio a la persona jurídica y a sus asociados, ya que aún si ha sido cometido por cualquiera de las personas mencionadas en el numeral 1, generare beneficio a un tercero ajeno a la persona jurídica, constituye un eximente de responsabilidad, al tenor de lo que establece el último inciso del Art. 49 arriba referido.

El presupuesto establecido en el último numeral, esto es el beneficio de un tercero excluiría de cualquier responsabilidad penal a la entidad bancaria frente al delito informático de apropiación ilícita ya que como se ha manifestado en reiteradas ocasiones, el beneficiado en este tipo de delitos es un tercero ajeno al banco y al cliente.

2.4.- ANÁLISIS DE LAS RESOLUCIONES INTERINSTITUCIONALES 001 – FGE – SBS – 2011 y 002 – FGE – SBS – 2011

EMITIDAS POR LA FISCALÍA GENERAL DEL ESTADO y LA SUPERINTENDENCIA DE BANCOS Y SEGUROS.-

En los años 2010 y 2011 en el Ecuador fueron presentadas en la Fiscalía General del Ecuador innumerables denuncias por personas que habían sido víctimas de distintos delitos informáticos, de manera particular aquellos relacionados con la apropiación indebida de fondos.

Las denuncias en mención tenían como denominador que los denunciantes eran clientes de la banca.

Frente a estas denuncias que sobrepasaron el número de mil quinientas en el año 2011 con un perjuicio de tres millones y medio de dólares, la Fiscalía General del Estado en colaboración de la Superintendencia de Bancos conformaron una comisión para investigar el aumento de los fraudes informáticos que afectaban a los clientes de la banca, comisión que realizo un análisis de los casos respecto de los siguientes puntos:

1) Si los Bancos daban cumplimiento a lo dispuesto en los Arts. 4 y 8 de la Ley de Defensa del Consumidor, en concordancia con lo establecido en los Arts. 20 y 21 del Reglamento de la Ley de Comercio Electrónico.

Los artículos invocados de la Ley de Defensa del Consumidor hacen referencia a los derechos del consumidor, entre ellos: derecho a la información adecuada; derecho a la educación del consumidor; derecho a la reparación e indemnización de daños y perjuicios por deficiencia en la calidad de bienes y servicios; derecho a acceder a mecanismos efectivos para la tutela administrativa y judicial de sus derechos.

Por su parte el reglamento de la Ley de Comercio Electrónico se refiere en las disposiciones mencionadas a la información que debe ser proporcionada al usuario de servicios electrónicos y a la seguridad en la prestación de éstos, estableciendo que se consideran datos sensibles del consumidor su información personal, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

2) Si las instituciones que debían ser analizadas podían comprobar que tenían alertas de control interno para prevenir fraudes.

3) Si las instituciones bancarias ante reclamos por fraudes informáticos contaban con procesos internos y si éstos cumplían las disposiciones emanadas de la Superintendencia de Bancos.

4) Si demostraban en los procesos de investigación de reclamos del cliente una adecuada información del avance de ésta**.**

5) Si las entidades bancarias mantenían provisión de riesgos en caso de fraudes informáticos.

6) Cuáles eran las soluciones a corto, mediano y largo plazo implementadas por las instituciones bancarias para minimizar el fraude informático. [111]

Luego del análisis de la investigación lo que sucedió es que la Fiscalía y la Superintendencia de Bancos representadas por sus máximos personeros suscribieron la resolución interinstitucional 001 – FGE – SBS – 2011 el 20 de Marzo del año 2011.

Las principales consideraciones que constan en la resolución (ANEXO II) del presente trabajo, fueron en resumen las siguientes:

- Que de conformidad con el Art. 226 de la Constitución de la República del Ecuador, las instituciones, organismos y dependencias del Estado debían coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución; que las actividades financieras eran un servicio de orden público que tenían la finalidad fundamental de preservar los depósitos;

[111] Santiago Acurio del Pino, *Fundamentos de la Responsabilidad de las Instituciones Financieras frente al Delito de Fraude Informático* (Apropiación Ilícita), Universidad Andina Simón Bolívar, 2012, p.22.

- Que el Art. 52 de la Constitución establece que las personas tienen derecho a disponer de bienes y servicios de óptima calidad, así como una información adecuada, clara, veraz, oportuna y completa sobre los servicios ofrecidos en el mercado, incluyendo los riesgos que pudieren prestar.

- Que la Constitución establece la responsabilidad civil y penal por la deficiente prestación de un servicio.

- Que la responsabilidad "es una situación jurídica en la que el patrimonio de una persona natural o jurídica debe responder para resarcir por una lesión producida a un tercero, atribuible a ésta, por un acto doloso, negligente o simplemente por la omisión de su deber o el riesgo creado. Como resultado del daño causado se genera una obligación de resarcimiento o reparación integral material o inmaterial".

- Que la banca había omitido su deber de protección de los depósitos de los clientes bancarios lo que había producido un daño en el patrimonio de estos últimos y que por lo tanto existía un nexo causal entre estos dos hechos. En este punto se especificó que la omisión del banco consistió en no informar a los clientes de los riesgos que existía al usar el servicio de banca el línea y que si el banco es el responsable de la seguridad del sitio web y de informar de uso correcto del sitio, debía brindar la información adecuada, veraz, clara, oportuna y completa procurando la educación del usuario con el objetivo de que éste haga un uso responsable del servicio.

- Que la responsabilidad es aquella situación jurídica podía originarse por un acto doloso, negligente o simplemente por la omisión de su deber y el riesgo creado, ya que se concluyó que existían falta de seguridad en los mecanismos de identificación del cliente para acceder a la plataforma interna, en otras palabras que el cliente cuando realizaba operaciones bancarias por internet lo hacía sin una información adecuada.

En atención a las consideraciones mencionadas se dictó una resolución desarrollada en ocho artículos, en los que:

a) Se dispuso que las instituciones del sistema financiero inicien correctivos para impedir el cometimiento tanto del delito de fraude informático como de los delitos relacionados con lavado de activos.
b) Se concluyó que la banca era responsable directa e indirectamente por los fraudes informáticos sufridos por sus clientes.
c) Se dispuso que las instituciones del sistema financiero "reconozcan" a sus clientes perjudicados por delitos de fraude bancario entre el período comprendido del 1ro de enero del 2010 hasta el 21 de marzo del 2011, según el monto reclamado.

   Así a los clientes que habían sufrido pérdidas de un dólar hasta dos mil dólares se les restituiría el cien por ciento; a los clientes que habían sufrido pérdidas de dos mil un dólar hasta diez mil dólares se les restituiría el ochenta por ciento; y a los clientes que habían sufrido pérdidas de más de diez mil dólares se le restituiría el sesenta por ciento.
d) Se dejó a salvo el derecho de las personas que no querían aceptar los montos señalados para seguir las acciones correspondientes.
e) Se notifico a las entidades bancarias que debían cumplir con lo dispuesto para que realicen el reintegro correspondiente a las personas que habían presentado sus reclamos.
f) Se dispuso que la Superintendencia de Bancos eleve en consideración a la Junta Bancaria para que ésta requiera a las instituciones financieras privadas la contratación de una póliza de fidelidad bancaria que incluya la cobertura delito informático y cibercrimen.

Para complementar la resolución examinada, el 25 de Abril del año 2011, la Superintendencia de Bancos y la Fiscalía General del Estado, por intermedio de sus máximos personeros firmaron una nueva resolución, signada con el número 002 – FGE – SBS – 2011, en la que se estableció:

g) Que para viabilizar el reintegro de los valores determinados en la resolución 001– FGE – SBS – 2011 se requería que las personas beneficiadas por ésta

firmen un acta de conformidad con las respectivas entidades bancarias mediante la que se liberaba al banco pagador y a sus funcionarios de cualquier otro nuevo reclamo sobre los hechos materia del reclamo originario.

h) La Superintendencia de Bancos se obligó a emitir normas que enfaticen la responsabilidad de los clientes por sus actos y omisiones en el manejo de claves secretas y la obligación de utilizar sistemas informáticos seguros para sus transacciones electrónicas.

Quienes idearon la emisión de las dos resoluciones arriba singularizadas se fundamentaron no solo en la consideración de que las actividades financieras son un servicio de "orden público" sino en la facultad de control que ejerce la Superintendencia de Bancos y Seguros, según el Art. 213 de la Constitución de la República.

Recordemos que en la primera parte de este capítulo se realizó un análisis de los términos "servicio público" y "servicio de orden público", éste último utilizado en el Art. 308 de la Constitución de la República para referirse a la actividad bancaria, calificación que si bien desde el punto de vista analizado no es apropiada, resultó adecuada para la emisión de las resoluciones interinstitucionales emitidas por la Fiscalía general del Estado y la Superintendencia de Bancos, ya que el Art. 54 de la Constitución de la República establece: "Las personas o entidades que presten servicios públicos o que produzcan o comercialicen bienes de consumo, serán *responsables civil* y penalmente, por la deficiente prestación der servicio, por la calidad defectuosa del producto, o cuando sus condiciones no estén de acuerdo con la publicidad efectuada o con la descripción que incorpore…". Esta disposición fue invocada para la determinación de la responsabilidad objetiva que se imputó a las entidades bancarias.

En conclusión, fueron las dos normas constitucionales mencionadas las que permitieron la emisión de las dos resoluciones detalladas, pero de la simple lectura de la segunda norma citada en el párrafo anterior se infiere que se habla de ***responsabilidad civil*** que es producto de un proceso judicial que permita determinarla y no de un acto

administrativo que imponga "reparaciones" sin haber dado a una de las partes la posibilidad de defenderse.

En las resoluciones en mención, por otra parte, se vinculó la potestad de vigilancia y control de la Superintendencia de Bancos y Seguros con los derechos del consumidor consagrados en la Ley Orgánica de Defensa del Consumidor ante todo aquellos referentes:

1.- A los derechos de los clientes y usuarios de la banca a que en los contratos de banca en línea no se utilicen cláusulas abusivas;

2.- A la educación financiera que debían haber recibido los clientes bancarios por parte de las instituciones bancarias para el uso de los servicios de la banca electrónica;

3.- A la obligación de la Banca, por intermedio de sus directivos, de proporcionar educación financiera a sus clientes; y[112],

4.- Al derecho de preservar los datos del cliente considerando las claves de seguridad que maneja para ingresar al sistema de banca en línea dentro de lo que se conoce como "derecho de autodeterminación informativa". [113]

Se manifestó así que las claves de ingreso a los servicios de banca en línea formaban parte del derecho de autodeterminación informativa y constituían "datos sensibles" del consumidor, entendidos éstos, de conformidad con lo que establece el Art. 21 del Reglamento de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos como "sus datos personales, información financiera de cualquier tipo como

[112] En este punto se concluyo que, los directivos de los bancos, de conformidad con lo establecía el Art. 30 de la Ley de Instituciones del Sistema Financiero eran responsables civil y penalmente por sus acciones y omisiones que deberían ser examinadas no solo a la luz de la referida ley sino de todo el ordenamiento jurídico, estableciendo que era atribución de éstos brindar información financiera a los clientes del banco por lo que al no hacerlo violentaron dicha norma.

[113] El derecho de autodeterminación informativa hace referencia a la prerrogativa que todo individuo tiene frente a cualquier ente público o privado, por la cual nadie debe introducirse, sin autorización expresa (de él mismo o por mandato de ley o judicial), en aquellos aspectos que no son públicos –sino de su vida personal, familiar, documentos, correspondencia y domicilio–, para conocerlos, conservarlos, procesarlos y/o transmitirlos, independientemente de que dicha acción le cause o no, algún daño o molestia.

números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Como un punto omitido en las resoluciones se encuentra la responsabilidad del prestador del servicio electrónico, recordando para el efecto, que el banco al contratar éste a otra persona, al igual que el cliente son usuarios del internet, de lo que se infiere que para la determinación de responsabilidades del modo que se lo hizo, es decir desde el punto de vista del Derecho del Consumidor, se debió también considerar como responsables al prestador del servicio en mención a favor de la banca, determinando la cadena de solidaridad de todo aquel que haya influido en un daño, tanto más cuanto que el Art. 50 de la Ley de Comercio Electrónico obliga a los proveedores en mención a informar sobre el servicio prestado.

Las resoluciones analizadas tuvieron defensores y detractores. En defensa de su legalidad encontramos el siguiente criterio esgrimido por el Dr. Santiago Acurio del Pino:

> "Es así que la omisión en este caso de las instituciones bancarias a través de sus directivos y demás subordinados presupone siempre la existencia de un determinado sistema de relaciones sociales del cual surge la exigencia de que los funcionarios bancarios en determinadas condiciones, mismas que están señaladas en el ordenamiento jurídico…como contractualmente lleven a cabo determinadas acciones, en este caso particular custodiar con responsabilidad los valores depositados en cada una de las instituciones bancarias, depósitos generados en cada una de las instituciones bancarias, depósitos generados por la confianza que los ciudadanos tienen en el servicio que el sistema financiero presta como servicio público, y que se ve defraudado por la laxitud de los controles y la falta de medidas preventivas eficaces y personalizadas que evitan como ya se mencionó esta clase de comportamientos que trasladan toda la responsabilidad al usuario del sistema financiero, dando lugar a una suerte de imputación de responsabilidad

subjetiva en la que se necesita la demostración y comprobación de la conducta culposa y dolosa del agente para hacerlo responsable del hecho, situación que no ocurre ya que esta afirmación de responsabilidad solamente queda sentada en el papel que el banco entrega negando el reclamo."[114]

Por otra parte la principal critica a las resoluciones se originaron en el sector bancario por las siguientes razones:

1.- El estado de indefensión que causó las resoluciones materia de análisis para los bancos irrespetó el derecho consagrado en el literal a) del numeral 7 del Art. 76 de la Constitución de la República, aplicable a todo procedimiento.

Como se manifestó, el antecedente inmediato para la expedición de las resoluciones fueron las numerosas denuncias presentadas por los clientes de la banca por fraudes informáticos, dichas denuncias originaron la apertura de una indagación previa dentro de la que las partes intervinientes, entre éstas las entidades bancarias podían presentar elementos de descargo. Como se infiere de la lectura de las resoluciones por otra parte también ante la Superintendencia de Bancos los perjudicados habían presentado reclamos, es decir que en el transcurso de dichos procesos penales y administrativos fueron dictadas las resoluciones que sin duda alguna dieron fin a éstos, a pesar de que se dejó a salvo el derecho de las instituciones financieras de ejercer acciones legales en contra de quienes cometieron los delitos de fraude informático.

Es así incorrecto que ignorando los procedimientos que se estaban llevando a efecto y otros que se debieron seguir, se haya establecido la responsabilidad de un conjunto de personas jurídicas sin haberles otorgado el derecho a la defensa y sobre todo sin siquiera haber considerado que cada caso pudo haber sido distinto, a pesar que en la segunda resolución en mención se determinó que los reintegros de dinero que debían

[114] Santiago Acurio del Pino, *Fundamentos de la Responsabilidad de las Instituciones Financieras frente al Delito de Fraude Informático* (Apropiación Ilícita), p.20.

realizar las instituciones financieras a sus clientes “no significaba en modo alguno reconocimiento de responsabilidad”.

2.- La falta de fundamento jurídico de las resoluciones es otra de las críticas, ya que como habíamos analizado, en nuestra legislación prima la responsabilidad subjetiva, amparada en normas tanto civiles como de defensa del consumidor, normas que para el juzgamiento de las entidades bancarias frente al cometimiento de delitos informáticos que afecten a sus clientes se encontraban vigentes a la fecha en la que se dictaron las resoluciones analizadas.

Aplicar la teoría de la responsabilidad objetiva contradice el respeto al ordenamiento jurídico, tanto más cuanto que para el juzgamiento de las entidades bancarias frente al cometimiento de delitos informáticos que afecten a sus clientes la ley prevé otro tipo de responsabilidad como se ha expuesto.

De la lectura del texto de las resoluciones se infiere que cuando se trata el tema de la responsabilidad civil no se cita las disposiciones legales que fueron consideradas para emitir éstas.

3.- La legitimidad de la actuación de la Fiscalía General del Estado y de la Superintendencia de Bancos y Seguros se encuentra avalada por la Constitución de la República, que no pueden ser desatendidas a pretexto de inexistencia de normas menores.

Al respecto, es necesario recordar que la Banca advertía antes de que se dicten las resoluciones, la problemática que hemos analizado en este trabajo, afirmación que la realizo sobre la base del contenido del boletín informativo 007 del mes de febrero del año 2011 de la Asociación de Bancos Privados del Ecuador, en el que se manifestó:

> “Con alguna frecuencia se esgrimen argumentos poco sólidos para endosar exclusivamente a la Banca la obligación de la seguridad en el uso de canales

> electrónicos, cuando se conoce que debe haber corresponsabilidad de las partes, en el buen uso de las herramientas electrónicas. La Banca privada seguirá sumando esfuerzos para incrementar la seguridad en sus canales transaccionales, fortaleciendo y difundiendo campañas de educación financiera, pero a la vez espera que las autoridades del Estado asuman también su papel objetivo y mesurado, al momento de evaluar las acciones que pudieran continuar llevándose a cabo en este tema"[115]

Si las entidades bancarias en su conjunto advertían de las consecuencias sociales y económicas que se estaban dando, a mi forma de entender los que debieron dar una solución al problema fueron las entidades bancarias, evitando de este modo que el Estado intervenga para solventar un problema que era competencia de éstas como depositarias del ahorro de los ciudadanos, es decir, desde mi punto de vista debieron ser como instituciones de derecho privado que prestan un servicio de interés público las llamadas a buscar una solución global al problema que advertían, de tal modo que yo diría que las resoluciones obligatorias y sancionatorias dictadas por la Fiscalía General del Estado en conjunto con la Superintendencia de Bancos no fue legales, por falta de fundamentación jurídica pero si legítimas.

Después de que han transcurrido más de tres años desde que se emitieron las resoluciones interinstitucionales, las causas que originaron el problema no han variado, según una publicación del Diario El Comercio, sino que los delitos informáticos que afectan a los clientes de la Banca han aumentado, así por ejemplo del delito de apropiación ilícita de datos personales que en el año 2010 existieron 903 denuncias aumentaron al año 2013 a 1380 denuncias. [116]

[115] Asociación de Bancos Privados del Ecuador, *Seguridad Electrónica: Una responsabilidad compartida*, Boletín Informativo de la Asociación de Bancos Privados del Ecuador, No 007 de Febrero del 2011, http://www.asobancos.org.ec/internas.asp?opcion=publicaciones.htm, Revisado en Agosto del 2014.

[116] Sara Ortiz, "El 63% de delitos cometidos en Internet tiene una sanción penal", El Comercio (Quito), 29 de junio 2014, 2.

Frente a esta problemática son evidentes tres soluciones que se han originado en los correspondientes estamentos estatales:

La primera, relacionada con la expedición del COIP en el que ya se sancionan de manera específica los delitos informáticos de apropiación ilícita que afectan a los clientes de la Banca, sin embargo cabe resaltar, como se manifestó al inicio del trabajo, que muchas veces este tipo de delitos trascienden fronteras por lo que para que la normativa promulgada tenga efecto deben a la par implementarse otro tipo de gestiones como la práctica de peritajes inmediatos y actos urgentes que permitan por ejemplo recuperar los registros y mensajes de datos existentes dentro de un equipo informático o que ayuden a establecer direcciones de IP, peritajes a través de los que se pueda preservar las evidencias y vestigios de la infracción tomando en cuenta que el principal obstáculo es dar con los autores de ésta por la forma en la que operan.

La segunda relacionada con el hecho de que la Superintendencia de Bancos, en cumplimiento de la resolución interinstitucional 001 – FGE – SBS – 2011 el 20 de Marzo del año 2011 ha conminado a las entidades bancarias la contratación de una póliza de fidelidad bancaria que incluya la cobertura delito informático y cibercrimen, lo cual lo ha realizado mediante la Resolución publicada en el Registro Oficial 635 de fecha 07 de Febrero del 2012, por la que se incluyo el Articulo 41 dentro del Título II denominado “De la Organización de las instituciones del sistema financiero privado”, título contemplado dentro del capítulo I del Libro I denominado “Normas para la aplicación de la Ley General de Instituciones del Sistema Financiero.

El Art. 41 agregado tiene el siguiente texto:

> “Art. 41.- Las instituciones financieras contratarán anualmente con las compañías de seguro privado, coberturas que aseguren a la entidad contra fraudes generados o a través de su tecnología de la información, sistemas telemáticos, electrónicos o similares, como mínimo ante los siguientes riesgos:

41.1.- Alteraciones de bases de datos;

41.2.- Accesos a los sistemas informáticos y de información de forma ilícita;

41.3.- Falsedad Informática;

41.4.- Estafa Informática;

41.5.- Daño Informático; y,

41.6.- Destrucción a la infraestructura a las instalaciones físicas necesarias para la transmisión, recepción o procesamiento de información"

Para implementar lo dispuesto en la resolución se otorgó como fecha tope a las instituciones financieras el 30 de Junio del año 2012.

La tercera, ha sido la expedición de la resolución JB – 2012 – 2148 de fecha 26 de Abril del 2012 por parte de la Junta Bancaria que estableció una serie de disposiciones que la banca debía implementar en plazos establecidos hasta 36 meses, para blindar los servicios de banca en línea contra fraudes informáticos, entre ellos la adopción de protocolos, pruebas anuales de vulnerabilidad y penetración de equipos, dispositivos y medios de comunicación, emisión de informes de dichas pruebas, mecanismos internos de control que reduzcan la posibilidad de que los clientes accedan a páginas web falsas, implementación de mecanismos de seguridad, implementación de mecanismos para impedir las copias de las páginas web de los bancos, mecanismos de autentificación de claves y contraseñas que contemplen tres factores, entre otros. Lo importante en la adopción de estas medidas es que para efectos de la determinación de culpabilidad las propias autoridades administrativas cuentan con parámetros para determinar si la banca cumplió o no con las exigencias estatales.

En la esfera privada los Bancos sí han tratado de realizar campañas informativas para que sus clientes no sean víctimas de delitos informáticos, basta ingresar a las páginas web que mantienen las entidades bancarias para percatarse que en éstas existe información de los delitos de los que pueden ser victimas los clientes bancarios en el uso de banca en línea y la consiguiente mensaje de alerta que se da para que éstos mantengan las precauciones necesarias; dicha campaña por otra parte también ha sido

implementada por la propia Superintendencia de Bancos y Seguros a través del portal del usuario financiero.

CONCLUSIONES Y RECOMENDACIONES

1.- El delito informático comprende una amplia gama de tipos penales, de éstos los principales que afectan a la banca privada son aquéllos denominados "fraudes informáticos" en los que se encuentra inmerso el delito de apropiación ilícita de fondos, que sí se encontraba tipificado en el extinto Código Penal.

2.- En el Ecuador, las principales modalidades que se presentan dentro de la apropiación ilícita de fondos por medios informáticos son el pharming y el phishing, que a partir de la expedición del Código Orgánico Integral Penal se encuentran contemplados como delitos.

3.- Las entidades bancarias al igual que sus clientes son víctimas frente a los delitos informáticos de apropiación ilícita, ya que estos delitos son cometidos en la mayoría de casos por personas extrañas a la entidad bancaria, sin embargo en virtud del riesgo operacional las primeras son las obligadas aminorar la existencia de éste, brindando la tecnología de la información adecuada que le permita al cliente acceder a servicios de banca en línea seguros.

4.- A partir de la Constitución expedida en el año 2008 se considera a la actividad bancaria como un servicio de orden público, concepto este extraño a dicha actividad que es netamente privada y que tiene un *interés público*.

5.- La responsabilidad civil de la banca a favor de sus clientes frente al delito informático de apropiación ilícita de fondos es una responsabilidad contractual ya que nace de la celebración con el cliente de un contrato denominado servicios de banca en línea, excluyendo a otros usuarios que sin haber pactado con el banco hacen uso de otros servicios bancarios.

6.- La responsabilidad civil de la banca a favor de sus clientes frente al delito informático de apropiación ilícita de fondos es una responsabilidad que tiene la característica de subjetiva en la que confluyen tres elementos básicos: a) la existencia de la culpa por parte de la entidad bancaria; b) la existencia del daño patrimonial sufrido por el cliente; y, c) la existencia del nexo causal entre la culpa y el daño patrimonial.

La responsabilidad objetiva es decir aquella en la que se prescinde del elemento culpa para dar importancia al daño sufrido, no puede ser aplicada para proteger al cliente de la banca frente al delito informático ya que en nuestro país no existe un fundamento legal para ello**,** ya que dicha responsabilidad es ajena al ámbito contractual**.**

7.- Las entidades bancarias ante sus clientes frente al delito de apropiación ilícita de fondos responden por culpa leve en virtud de que se reputa que el contrato de banca en línea acarrea beneficio para las dos partes que los suscriben, ello en virtud de lo determinado en el primer inciso del Art. 1563 del Código Civil.

8.- En los procesos judiciales a seguirse por parte de los clientes en contra de los bancos para determinar la responsabilidad civil de éstos frente al delito informático, el onus probandi corresponde a la banca ya que según el último inciso del Art. 1563 del Código Civil "la prueba de la diligencia o cuidado incumbe al que debía emplearlo".

En el caso que nos ocupa el banco es el obligado a implementar una plataforma tecnológica adecuada que le permita hacer uso a los clientes de los servicios de banca en línea de manera segura. Por tanto, en un eventual proceso judicial, es al banco al que le incumbe probar que en efecto lo hizo.

9.- En el Ecuador no existe responsabilidad penal de los bancos por los delitos informáticos de apropiación ilícita de fondos de los que sus clientes son víctimas por no encontrarse tipificado en el COIP y porque tampoco es aplicable la figura de la comisión por omisión, desde mi punto de vista.

10.- Las resoluciones interinstitucionales 001 – FGE – SBS – 2011 Y 002 – FGE – SBS – 2011 emitidas por la Fiscalía General del Estado y la Superintendencia de Bancos y Seguros, fueron expedidas frente a la gran cantidad de denuncias por delito informático de apropiación ilícita de fondos cometidos contra los clientes bancarios en el año inmediato anterior a su expedición, luego de una investigación que se realizó dentro de las entidades bancarias referente a los procesos internos que se habían dado en los bancos ante las reclamaciones de sus clientes. En estas resoluciones se aplicó el criterio de la responsabilidad objetiva, que no rige en nuestro ordenamiento jurídico para las relaciones contractuales que surgen entre una entidad bancaria y sus clientes.

11.- Si admitimos que la responsabilidad objetiva aplicada en las resoluciones interinstitucionales 001 – FGE – SBS – 2011 y 002 – FGE – SBS – 2011 emitidas por la Fiscalía General del Estado y la Superintendencia de Bancos y Seguros no fue apropiado, estaríamos frente a una actuación ilegal, empero si admitimos que las afirmaciones realizadas en los considerandos expuestos en las resoluciones y que motivaron su expedición son ciertas resultarían legítimas, de manera particular por la falta de accionar de las entidades bancarias frente a los perjuicios sufridos por sus clientes, ya que no tomaron las medidas adecuadas y oportunas para frenar el problema de los fraudes informáticos ni les dieron a los perjudicados una solución oportuna y eficaz.

12.- Se han adoptado medidas para aminorar el riesgo operacional que tiene la entidad bancaria y sus clientes frente al delito informático de apropiación ilícita entre ellas la obligación de los bancos de contratar seguros privados que contengan coberturas a la entidad contra fraudes generados por medios informáticos y la obligación de implementar una serie de medidas técnicas que han sido reguladas por parte del órgano de control del Estado, mientras que por otra parte se ha procurado por parte de las entidades bancarias publicitar educación financiera en favor de sus clientes.

Recomendaciones.-

Si bien el COIP ha tipificado las conductas delictivas de pishing y pharming ello no soluciona el problema mientras no se adopten medidas complementarias que impidan que tales delitos se cometan en pos de buscar soluciones a las causas y no a las consecuencias de un problema como el analizado, es por ello que:

1.- Los servicios de Banca en línea deben ser personalizados, es decir según las necesidades de cada cliente, de tal modo que tanto la entidad bancaria como el cliente blinden todo tipo de acciones delictivas que les perjudiquen, no sería ambicioso entonces pensar que el banco implemente a los clientes que lo soliciten software especiales en los equipos que utilice el cliente (ya sea computadores, tablets o teléfonos) desde los cuales los clientes accedan al servicio en mención.

2.- Si bien hablar de reformas legales resulta también ambicioso diré que sí se requiere que la responsabilidad que los bancos tienen frente ante sus clientes que han sido víctimas del delito informático de apropiación ilícita de fondos sea objetiva bien valdría la pena que en un cuerpo legal, llámese Ley de Defensa del Consumidor, Código Civil, así se establezca a fin de que existan normas que regulen esta situación en específico, lo cual sería beneficioso desde el punto de vista de la seguridad jurídica.

3.- Por otra parte el estudio del delito informático me lleva a concluir y recomendar que siendo este un delito que entre sus principales características se encuentra la transnacionalidad, se debe procurar tener una legislación común que permita a los Estados con agilidad actuar frente a éste tipo de delincuencia.

4.- No está por demás recomendar a los propios Bancos más allá de que cumplan con las adecuaciones necesarias para el ofrecimiento del servicio de banca en línea que sean ellos los como principales perjudicados los que activen el aparato jurisdiccional para perseguir este tipo de delitos que afectan a sus clientes.

BIBLIOGRAFIA

1.- Acurio del Pino, Santiago. Fundamentos de la Responsabilidad de las Instituciones Financieras frente al Delito de Fraude Informáico (Apropiación Ilícita); Universidad Andina Simón Bolívar; 2012.

2.- Alessandri, Arturo. Obligaciones, s.p.a.

3.- Alvarado, Haydeé. Derecho del Consumidor; primera parte; texto guía; Loja; Editorial de la Universidad Técnica Particular de Loja, 2006.

4.- Alvarez, Rubio Julio. Derecho de Obligaciones; Obra Jurídica Enciclopédica; México; Editorial Porrúa; 2012.

5.- Araujo, Granda Paulina. La Nueva Teoría del delito Económico y Empresarial en el Ecuador; Quito; Coorporación de Estudios y Publicaciones.

6.- Arias Torres, Luis Bramont. El Delito Informático en el Código Penal Peruano; Biblioteca de Derecho Contemporáneo; Vol 6.

7.- Barbier, Eduardo Antonio. La Contratación Bancaria; Buenos Aires; Editorial Astrea; 2000.

8.- Cortes, Edgar. La culpa contractual en el sistema jurídico latinoamericano; Bogota; Editorial Salamanca; 2001.

9.- Derecho Informático e Informática Jurídica; Varios autores; México; Editorial Porrua; 2012.

10.- Ettore, Gianantonio. Informática y Derecho; Volumen 3; Tranferencia Electrónica de Fondos y Autonomía Privada; Buenos Aires; Ediciones Depalma; 1997.

11.- Herrmann Fernández, Patricia. Comercio Electrónico; Loja; Editorial de la Universidad Técnica Particular de Loja; 2006.

12.- Jimenez de Asua, Luis. Principios del Derecho Penal; La ley y el delito; 4ta edición; Buenos Aires; Editorial Sudamericana; 2005.

13.- Kabas de Martorell, María Eliza. Tratado de Derecho Bancario; Tomo I; Buenos Aires; Rubinzal- Culzoni Editores; 2011.

14.- Paéz Rivadeneira, Juan Jose y Acurio del Pino, Santiago; Derecho y Nuevas Tecnologías; Quito; Corporación de Estudios y Publicaciones; 2010.

15.- Pardo Iranzo, Virginia. Ejecución de Sentencias por obligaciones de hacer y de no hacer; Valencia; Tirant lo Blanch; 2001.

16.- Peña Valenzuela, Daniel. Responsabilidad Civil en la era digital; Bogotá; Proyectos Editoriales Curcio Penen; 2007.

17.- Piaggio, Luccas A. La Banca como servicio público; una ficción legal contra natura; Federación Latinoamericana de Bancos FELABAN; 2010.

18.- Pizarro Ramon, Daniel. Responsabilidad Civil por el Riesgo o Civil de las cosas; Buenos Aires; Editorial Universidad; 1983.

19.- Política y Derecho de Consumo; Varios autores; Bogota; El Navegante Editores; 1998.

20.- Responsabilidad de los Bancos frente al cliente; varios autores; Buenos Aires; Rubinzal- Culzoni Editores; 2006.

21.-Rojas Franco, Enrique. Derecho Administrativo y Derecho Procesal Administrativo; Guayaquil; Edilex S.A.; 2007.

22.- Rovira del Canto, Enrique. Delincuencia informática y fraudes informáticos; Granada; Editorial COMARES; 2002.

23.- Salamea, Carpio Diego. El Delito Informático y la Prueba Pericial Informática; Quito; Editorial Jurídica del Ecuador; 2013.

24.- Salas Peña, Daniela. Responsabilidad Civil Bancaria por delitos informáticos; Tesis de Grado; Costa Rica; 2009.

25.- Villegas, Carlos Gilberto. Contratos Mercantiles y Bancarios; Tomo II; Buenos Aires; Su Gráfica; 2005.

26.- Vizueta, Ronquillo Juan; Delitos Informáticos en el Ecuador; Guayaquil; Editorial Edino; 2011.

Publicaciones

Ortiz, Sara. El 63% de delitos cometidos en Internet tiene una sanción penal; El Comercio; Domingo 29 de Junio 2014; 2.

Leyes y Resoluciones

Constitución de la República

Código Civil

Código Penal

Código Integral Penal

Código de Transparencia y de Derechos del Usuario del Sistema Financiero expedido mediante resolución No JB – 2010 – 1782 de 19 de Agosto del 2010.

Ley de Instituciones del Sistema Financiero

Ley Orgánica de Defensa del Consumidor

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos

Reglamento de la ley Comercio Electrónico, Firmas Electrónicas y Mensajes de datos

Reglamento de la Ley de Cheques

Resolución JB – 2005 – 766.

Resolución JB – 2005 – 834

Resolución JB – 2010 – 1782

Resolución JB – 2012 - 2226

Resolución JB – 2012 – 2148

Resolución JB – 2012 – 2155

Resolución JB – 2013 – 2393.

Artículos encontrados en páginas WEB:

Jefferson (único nombre que identifica al autor de la pagina) Artículo de Informática Forense, Técnica del Salami, http://jeffersonforense.blogspot.com/2011/08/delitos-informaticos-tecnica-del-salami.html.

Banco del Pacífico, página web, https://www.bancodelpacifico.com/servicio-al-cliente/servicios/seguridad.aspx, 20 Octubre 2014.

Francisco Alvarez Valdez, Fraudes *Bancarios. Impacto en el resto de las Entidades del Sistema Financiero* , Mitigación del Riesgo y Sanciones Aplicadas, XXIX Congreso Latinoamericano de Derecho Financiero, 2010 http://www.felaban.com/archivos_actividades_congresos/11.pdf.

Deloitte, Riesgo Operativo, Resolución JB-2005-834, Estamos Listos? http://www.deloitte.com/view/es_ECcc/perpectivas/estudios-y-publicaciones/articulo.

Grando Jose y Medina Marcos. UNIVERSIDAD NACIONAL DEL NORESTE. Comunicaciones Científicas y Tecnológicas 2006. Facultad de Derecho y Cs. Sociales y Políticas (UNNE). Salta Nº 465- Código Postal 3400 – Corrientes Capital – República Argentina.http://www.unne.edu.ar/unnevieja/Web/cyt/cyt2006/01-Sociales/2006-S-066.pdf.

Asociación de Bancos Privados del Ecuador, ¿Los servicios Financieros, un servicio público?, Boletín Informativo Nro 37, 2014, http://www.asobancos.org.ec//ABPE_INFORMA/No37.PdF.

Mariana Fonseca Villanea, *El hecho de un tercero como eximente de la responsabilidad objetiva bancaria*, http://www.ulacit.ac.cr/files/careers/48_fonsecavillanea.pdf.

Temas de Derecho, *La Responsabilidad Civil*, http://temasdederecho.com/2012/06/04/la-responsabilidad-civil/.

Jaime Mendieta, La culpa *incontrahendo – Historia, Evolución y Estado Actual de la cuestión*, http://www.emercatoria.edu.co/PAGINAS/VOLUMEN10/HTML2/125.html.

José María Lescano, Análisis de la Responsabilidad Civil de los buscadores de Internet, http://sedici.unlp.edu.ar/bitstream/handle/10915/21019/Documento_completo.pdf?sequence=1.

Gladys Santana – Helem Sánchez y otro. Cuadro comparativo de la responsabilidad civil y penal. http://es.slideshare.net/helemaleja/cuadro-comparativo-rcc-vs-rce-rc-vs-rp.

Enciclopedia Jurídica. *Responsabilidad Objetiva*. http://www.enciclopedia juridica.biz14.com/d/responsabilidad-objetiva/responsabilidad-objetiva.htm. s.f.

Monografía

Acurio del Pino, Santiago. Fundamento de la Responsabilidad de las Instituciones Financieras frente al Delito de Fraude Informático (Apropiación Ilícita), Universidad Andina Simón Bolívar, 2012.

Jurisprudencia

Corte Suprema de Justicia, (Sentencia de casación: *Caso Delfina Torres vs PetroEcuador*, expediente número 229 – 2002), publicado en el R.O. Nro.43 de 19 de marzo del 2003.

ANEXO UNO

DELITOS INFORMATICOS

UBICACIÓN CODIGO PENAL – COIP

DELITO	**CODIGO PENAL**		**CODIGO INTEGRAL PENAL**	
	Ubicación	**Texto**	**Ubicación**	**Texto**
INVIOLABILIDAD DE SECRETOS (divulgación de secretos)	Libro II (Denominado Delitos en Particular) Título II (Delitos contra las garantías constitucionales y la igualdad racial) Capítulo V (Delitos contra la Inviolabilidad de Secreto)	"**Art. ..**- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica. Si la información obtenida se refiere a	Titulo IV (Denominado Infracciones en general) Capítulo III (Delitos contra los derechos del buen vivir) Sección Tercera (Delitos contra la seguridad de los activos de los sistemas de información y comunicación)	**Artículo 229.- Revelación ilegal de base de datos.-** La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por

		seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica. La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la		una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

		información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. **Art. ..**- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.		
SABOTAJE INFORMATICO	Libro II (Denominado Delitos en Particular) Título III	"**Art. ...**- 262.- Serán reprimidos con tres a seis años de reclusión	Titulo IV (Denomina do Infracciones en general)	**Artículo 232.- Ataque a la integridad de sistemas informáticos.-**

	(Delitos contra la la Administración Pública) Capítulo V (Violación de los Deberes de Funcionarios Públicos, de la Usurpación de Atribuciones y de los Abusos de Autoridad)	menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.	Capítulo III (Delitos contra los derechos del buen vivir) Sección Tercera (Delitos contra la seguridad de los activos de los sistemas de información y comunicación)	La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que: 1.Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a

				causar los efectos señalados en el primer inciso de este artículo. 2.Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.
FALSIFICACION ELECTRONICA	Libro II (Denominado Delitos en Particular) Título IV (Delitos contra la Fé Pública) Capítulo III (Falsificación de Documentos en General)	"**Art. ...**- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier	**SUPRIMIDO**	**SUPRIMIDO** **Sin embargo en el Art. 186 que trata de la estafa, se lee como medio de cometer este delitos términos que implican falsedad como : clonación** **Artículo 186.- Estafa.-** La

		medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea: 1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial; 2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad; 3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho. El delito de		persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que: 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario. 2. Defraude mediante el uso de dispositivos

		falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.		electrónicos que alteren, modifiquen, **clonen o dupliquen** los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares. 3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica. 4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento. 5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor. La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a

				cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años.
ESPIONAJE INFORMATICO (DAÑOS INFORMATICO AL SOFTWARE)	Libro II (Denominado Delitos en Particular) Título V (Delitos contra la Seguridad Pública) Capítulo VII (Incendios y Otras Destrucciones)	**Art. ...**- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica. La pena de prisión será de tres a cinco años	Titulo IV (Denominado Infracciones en general) Capítulo III (Delitos contra los derechos del buen vivir) Sección Tercera (Delitos contra la seguridad de los activos de los sistemas de información y comunicación)	**Artículo 233.- Delitos contra la información pública reservada legalmente.-** La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la

		y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional. **Art. ...**- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos		seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

		dólares de los Estados Unidos de Norteamérica.		
APROPIACION ILICITA DE INFORMACION ELECTRONICA	Libro II (Denominado Delitos en Particular) Título X (Delitos contra la Propiedad) Capítulo II (Robo)	**Art. ...**- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas	Titulo IV (Denominado Infracciones en general) Capítulo II (Delitos contra los derechos de libertad) Sección Novena (Delitos contra el derecho a la propiedad)	**Artículo 190.- Apropiación fraudulenta por medios electrónicos.-** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de

		informáticos, telemáticos o mensajes de datos. **Art. ...**- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios: 1.Inutilización de sistemas de alarma o guarda; 2.Descubrimiento o descifrado de claves secretas o encriptadas; 3.Utilización de tarjetas magnéticas o perforadas; 4.Utilización de controles o instrumentos de apertura a distancia; y, 5. Violación de seguridades electrónicas, informáticas u otras semejantes.		uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.
ESTAFA	Libro II	Al Art. 563 se	Titulo IV	**Artículo 186.-**

ELECTRONICA	(Denominado Delitos en Particular) Título X (Delitos contra la Propiedad) Capítulo V (Estafa)	incorporó el último inciso: Art. 563.- El que con el propósito de apropiarse de una cosa perteneciente a otro, se hubiere hecho entregar fondos, muebles, obligaciones, finiquitos, recibos, ya haciendo uso de nombres falsos, o de falsas calidades, ya empleando manejos fraudulentos para hacer creer en la existencia de falsas empresas, de un poder, o de un crédito imaginario, para infundir la esperanza o temor de un suceso, accidente o cualquier otro acontecimiento quimérico, o para buzar de otro modo de la confianza o de la credulidad, será reprimido con prisión de seis meses a cinco años y multa de ocho a ciento cincuenta	(Denominado Infracciones en general) Capítulo II (Delitos contra los derechos de libertad) Sección Novena (Delitos contra el derecho a la propiedad)	**Estafa.-** La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que: 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario. 2. Defraude mediante el uso

		y seis dólares de los Estados Unidos de Norteamérica. **Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos**		de dispositivos electrónicos que alteren, modifiquen, **clonen o dupliquen** los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares. 3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica. 4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento. 5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor. La persona que perjudique a más de dos personas o el monto de su perjuicio sea

				igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años.
CONTRAVENCION	Libro Tercero Título I (Clasificación de las Contravenciones. Capítulo III (Contravenciones de Tercera Clase)	Art. 606.- Conductas y circunstancias típicas de las contravenciones de Tercera Clase.- Serán reprimidos con multa de siete a catorce dólares de los Estados Unidos de Norteamérica y con prisión de dos a cuatro días, o con una de estas penas solamente:… 19.- Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos	Pasa a ser delito que puede cometerse por medios informáticos. Titulo IV (Denominado Infracciones en general) Capítulo II (Delitos contra los derechos de libertad) Sección Sexta (Delitos contra el derecho a la intimidad personal y familiar)	**Artículo 178.- Violación a la intimidad.-** La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, **información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio**, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que

				divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

OTROS DELITOS INCORPORADOS AL CODIGO INTEGRAL PENAL RELACIONADOS CON MEDIOS INFORMATICOS

DELITOS	UBICACION	TEXTO
Pornografía con utilización de niñas, niños o adolescentes	Titulo IV (Denominado Infracciones en general) Capítulo III (Graves Violaciones a los derechos Humanos contra el Derecho Internacional Humanitario) Sección Tercera (Diversas formas de explotación)	**Artículo 103.- Pornografía con utilización de niñas, niños o adolescentes.-** La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años…
Contacto con finalidad Sexual con menores de dieciocho años por medios electrónicos	Titulo IV (Denominado Infracciones en general) Capítulo II (Delitos contra los derechos de libertad) Sección	**Artículo 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.-** La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno

	Novena (Delitos contra la integridad sexual y reproductiva)	a tres años. Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años. La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años. **Artículo 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.-** La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años.
Delitos contra el derechos a la identidad	Titulo IV (Denominado Infracciones en general) Capítulo II (Delitos contra los derechos de libertad) Sección Decima (Delitos contra el derecho a la identidad)	**Artículo 211.- Supresión, alteración o suposición de la identidad y estado civil.-** La persona que ilegalmente impida, altere, añada o suprima la inscripción de los datos de identidad suyos o de otra persona **en programas informáticos**, partidas, tarjetas índices, cédulas o en cualquier otro documento emitido por la Dirección General de Registro Civil, Identificación y de Cedulación o sus dependencias o, inscriba como propia, en la Dirección General de Registro Civil, Identificación y de Cedulación a una persona que no es su hijo, será sancionada con pena privativa de libertad de uno a tres años.
Interceptación Ilegal de Datos	Titulo IV (Denominado Infracciones en general) Capítulo III (Delitos contra los derechos del buen vivir) Sección Tercera	**Artículo 230.- Interceptación ilegal de datos.-** Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener

	(Delitos contra la seguridad de los activos de los sistemas de información y comunicación)	información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior
Transferencia Electrónica de activo patrimonial	Titulo IV (Denominado Infracciones en general) Capítulo III (Delitos contra los derechos del buen vivir) Sección Tercera (Delitos contra la seguridad de los activos de los sistemas de información y comunicación)	**Artículo 231.- Transferencia electrónica de activo patrimonial.-** La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.
Acceso no consentido a un sistema informático o de telecomunicaciones	Titulo IV (Denominado Infracciones en general) Capítulo III (Delitos contra los derechos del buen vivir)	**Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.-** La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho para explotar ilegítimamente

	Sección Tercera (Delitos contra la seguridad de los activos de los sistemas de información y comunicación)	el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagar losa los proveedores de servicios legítimos, será sancionada con la pena privativa dela libertad de tres a cinco años.
Delitos contra el Régimen de Desarrollo	Título IV (Denominado Infracciones en general)	**Art. 298.- Defraudación tributaria.-** La persona que simule, oculte, omita, falsee o engañe en la determinación de la obligación tributaria, para dejar de pagar en todo o en parte los tributos realmente debidos, en provecho propio o de un tercero, será sancionada cuando:.. 8. Altere libros o **registros informáticos** de contabilidad, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos.

ANEXO DOS

FISCALÍA GENERAL DEL ESTADO

RESOLUCIÓN INTERINSTITUCIONAL
No. 001-FGE-SBS-2011

Ab. Pedro Solines Chacón
SUPERINTENDENTE DE BANCOS Y SEGUROS

Dr. Washington Pesántez Muñoz
FISCAL GENERAL DEL ESTADO

CONSIDERANDO:

QUE, el artículo 194 de la Constitución de la República establece que la Fiscalía General del Estado tiene autonomía administrativa, económica y financiera, funciona de manera desconcentrada, y su máxima autoridad y representante legal es el Fiscal General;

QUE, la Superintendencia de Bancos y Seguros es un organismo técnico de vigilancia, auditoria, intervención y control de actividades financieras de la Banca Pública y Privada;

QUE, la norma constitucional determina que el titular de la acción penal y de la investigación pre procesal y procesal penal, de hechos que sean presumiblemente considerados delitos de acción pública, dentro del nuevo Sistema Procesal Penal Acusatorio, es el Fiscal;

QUE, la Superintendencia de Bancos y Seguros, debe velar porque las entidades sujetas a su control, actúen bajo el ordenamiento jurídico vigente y atiendan al interés general.

Este Organismo de Control ejercerá la supervisión, vigilancia y control del sistema financiero, con especial atención a **LA PROTECCIÓN DE LOS INTERESES DEL PÚBLICO;**

QUE, de acuerdo a lo dispuesto en el Art. 226 de la Constitución, las Instituciones del Estado, sus organismos, dependencias, tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo **EL GOCE Y EJERCICIO DE LOS DERECHOS RECONOCIDOS EN LA CONSTITUCIÓN**. Por este mandato de la Carta Fundamental, la Fiscalía General del Estado y la Superintendencia de Bancos y Seguros, ante el aumento de los Fraudes en el Sistema Informático a nivel nacional, han decidido en el ámbito de sus funciones coordinar acciones y conformar una Comisión para investigar estos hechos que revisten el carácter de delito, a fin de buscar una solución viable al perjuicio patrimonial que han sufrido varios usuarios del Sistema Financiero, por el cometimiento de este hecho ilícito, además de evitar que las transferencias fraudulentas de estos fondos sirvan para el cometimiento de delitos relacionados al lavado de activos en el país;

QUE, el Art. 426 de la Constitución menciona que todas las personas, autoridades e instituciones están sujetas a la Constitución. Por tanto la Fiscalía General del Estado y la Superintendencia de Bancos deben actuar en consecuencia y ceñidos a la norma constitucional, y velar por la aplicación directa de los derechos humanos reconocidos en ella sin que se pueda alegar falta de ley o desconocimiento de las normas para justificar la vulneración de derechos y garantías establecidos en la Constitución;

QUE, las actividades financieras son un servicio de **ORDEN PÚBLICO**, y podrán ejercerse, previa autorización del Estado, de acuerdo con la ley, tendrán la finalidad fundamental de **PRESERVAR LOS DEPÓSITOS** y atender los requerimientos de financiamiento para la consecución de los objetivos de desarrollo del país;

QUE, los perjudicados por los fraudes del sistema informático han acudido tanto a la Fiscalía General del Estado como a la Superintendencia de Bancos a fin de hacer valer sus derechos;

QUE, los servicios públicos que prestan las entidades financieras privadas, están sujetos al control de la Superintendencia de Bancos y su accionar está sometido al régimen legal de derecho público consagrado en la Ley de Instituciones del Sistema Financiero, que regula entre otros los contratos Bancarios, los mismos que establecen la relación jurídica entre el cliente y la entidad financiera la cual se crea normalmente a través de un contrato de cuenta corriente o cuenta de ahorros, que no es otra cosa que una acción mediante la cual el depositante transfiere el dinero al depositario, debiendo éste restituirlo cuando se le reclame. **LA OBLIGACIÓN LEGAL DE CUSTODIA** del depositario implica guardar y conservar el dinero objeto de depósito;

QUE, el Art. 52 de la Constitución señala que: *Las personas tienen derecho a disponer de* ***BIENES Y SERVICIOS DE ÓPTIMA CALIDAD,*** *así como a una información precisa, no engañosa, una* **INFORMACIÓN ADECUADA, VERAZ, CLARA, OPORTUNA Y COMPLETA** sobre los bienes y servicios ofrecidos en el mercado, así como sus precios, características, calidad, condiciones de contratación y demás aspectos relevantes de los mismos, incluyendo **LOS RIESGOS QUE PUDIEREN PRESTAR**; en igual sentido la Carta Magna dispone que *Las personas o entidades que presten servicios públicos o que produzcan o comercialicen bienes de consumo,* ***SERÁN RESPONSABLES CIVIL Y PENALMENTE POR LA DEFICIENTE PRESTACIÓN DEL SERVICIO,*** *por la calidad defectuosa del producto, o cuando sus condiciones no estén de*

acuerdo con la publicidad efectuada o con la descripción que incorpore, por tanto y dado que las actividades financieras son tanto **SERVICIO PÚBLICO** como un servicio de **ORDEN PÚBLICO**, se considera como **NO NEGOCIABLES. LA RUPTURA DEL ORDEN PÚBLICO** o **PUESTA EN PELIGRO** del servicio público da lugar a la imposición de una sanción dependiendo de la gravedad desde la administrativa, a la civil e inclusive la penal;

QUE, la Responsabilidad es aquella situación jurídica en la que el patrimonio de una persona natural o jurídica debe responder para resarcir por una lesión producida a un tercero, atribuible a ésta, por un acto doloso, negligente o simplemente por la omisión de su deber y el riesgo creado. Como resultado del daño causado se genera una obligación de resarcimiento o reparación integral material e inmaterial;

QUE, un elemento determinante para el surgimiento de la responsabilidad civil, es la omisión de proteger los depósitos de los clientes del sistema financiero, desatención que produce **UN DAÑO EN EL PATRIMONIO** de cuenta corrientitas y cuenta ahorristas, quienes han sido perjudicados por el fraude informático. Es así que **EL NEXO CAUSAL** se verifica entre estos dos hechos cuando el banco al **OMITIR SU DEBER DE PROTECCIÓN**, no le informa al cliente de los riesgos que existe al usar el servicio de banca en línea, si bien el cliente es responsable de las claves de acceso al sistema, el banco es responsable de la seguridad del sitio web y de informar al usuario el uso correcto del sitio, brindando para ello la información adecuada, veraz, clara, oportuna y completa procurando entonces la educación del usuario con la finalidad ulterior de que éste haga un uso responsable del servicio de banca en línea. Por tanto el banco no puede alegar la entera responsabilidad del usuario perjudicado por este delito, cuando **el banco es también responsable por la omisión de su obligación de preservar los depósitos de sus clientes como manda la Carta Fundamental.**

El desarrollo de servicios asumidos por las Instituciones Financieras, lleva implícito el deber de garantizar la seguridad de estos. **La falla en el funcionamiento del servicio que ofrece el intermediario financiero, radica en la falta de seguridad en los mecanismos de identificación del cliente para acceder a la plataforma interna.** Desde esta perspectiva, producto de los riesgos inherentes a la transmisión de datos mediante Internet, se deben **brindar las herramientas necesarias para reducir la posibilidad de que ocurra una suplantación de identidad.** Se trata de una característica intrínseca del servicio que ofrece el banco. En este sentido, la responsabilidad se imputa como

consecuencia del riesgo creado y la inseguridad que presenta el sistema; y,

En mérito de las consideraciones señaladas y en ejercicio de las facultades conferidas en la Constitución y en la Ley.

RESUELVEN:

Art. 1.- Las Instituciones del Sistema Financiero emprenderán acciones correctivas necesarias para impedir el cometimiento del denominado "fraude informático" y de los delitos relacionados con el lavado de activos.

Art. 2.- Las Instituciones del Sistema Financiero, realizarán campañas de información personalizada a sus clientes a fin de evitar que sean perjudicados por las transacciones a través del sistema informático.

Art. 3.- La Comisión conformada por funcionarios de la Fiscalía General del Estado y de la Superintendencia de Bancos y Seguros, han investigado las denuncias presentadas por usuarios, clientes de la banca privada, que han sido víctimas de la fragilidad del sistema informático por ella utilizado y que les ha ocasionado pérdidas en sus depósitos en cuentas aperturadas en las diferentes instituciones financieras del país, determinándose la responsabilidad directa o indirecta de éstas, por lo que la Comisión como resultado de las indagaciones y procesos de control practicados, recomienda y considera que los depositantes y usuarios que han resultado perjudicados deben recibir el resarcimiento de su patrimonio por parte de las instituciones bancarias, custodias de esos depósitos.

Art. 4.- Por lo señalado, las instituciones del Sistema Financiero del país reconocerán valores a sus clientes, que han sufrido pérdidas patrimoniales a consecuencia de la fragilidad y vulnerabilidad del Sistema Informático empleado (fraude informático), en el periodo comprendido entre el 1ro de Enero del 2010 hasta la presente fecha, según este cuadro:

MONTO RECLAMADO	% RESTITUIDO
De 1 USD a 2000 USD	100%
De 2001 USD a 10.000 USD	80%
Más de 10.000 USD	60%

La devolución de los dineros a los usuarios perjudicados, se hará de forma inmediata, por medio de transferencia bancaria a la cuenta corriente o de ahorros que los usuarios perjudicados posean en las correspondientes Instituciones Financieras del país.

Art. 5.- Si los usuarios perjudicados no aceptaren los montos señalados en esta Resolución, podrán seguir las acciones legales correspondientes a fin de reclamar el cien por ciento de su pérdida patrimonial.

Art. 6.- Las Instituciones Financieras Privadas, serán notificadas por parte de la Superintendencia de Bancos y Seguros con la presente Resolución y con el listado elaborado por la Comisión en el que se señalan los datos de las personas que aparecen como perjudicadas. La inobservancia de esta Resolución dará lugar a las sanciones previstas en la Ley de Instituciones del Sistema Financiero, sin perjuicio de las de orden civil y penal a que hubiere lugar.

Art 7.- La Superintendencia de Bancos y Seguros, elevará a consideración de la Junta Bancaria, se requiera a las Instituciones Financieras Privadas, la contratación de una "Póliza de Fidelidad Bancaria" que incluya la cobertura denominada "Delito Informático y Cibercrimen", que brinde amparo contra fraudes informáticos bajo condiciones pactadas entre los clientes y el Banco y que aseguren la cobertura necesaria sobre estos hechos y las exclusiones que se aplicarán, o la expedición de una normativa que persiga similar finalidad.

Art. 8.- La presente Resolución entrará a regir a partir de la presente fecha, y de su efectiva ejecución y cumplimiento encárguese la Superintendencia de Bancos y Seguros, en su calidad de Organismo de Control de las Instituciones Financieras.

Dado y firmado en Quito, Distrito Metropolitano, a los veinte y un días del mes de marzo del dos mil once.

Ab. Pedro Solines Chacón
SUPERINTENDENCIA DE BANCOS Y SEGUROS

Dr. Washington Pesántez Muñoz
FISCAL GENERAL DEL ESTADO

CER...

FISCALÍA GENERAL DEL ESTADO

RESOLUCION INTERINSTITUCIONAL No. 002-FGE-SBS-2011

Ab. Pedro Solines Chacón
SUPERINTENDENTE DE BANCOS Y SEGUROS

Dr. Washington Pesántez Muñoz
FISCAL GENERAL DEL ESTADO

CONSIDERANDO:

Que, la Superintendencia de Bancos y Seguros y la Fiscalía General del Estado, receptoras de denuncias presentadas por usuarios, clientes de la banca privada, que han sido víctimas de la fragilidad del sistema informático, emitieron el pasado 21 de marzo del 2011 la Resolución Interinstitucional No. 001-FGE-SBS-2011 en la cual se ordena la devolución de los dineros a los usuarios perjudicados por el delito de Apropiación Ilícita (fraude informático), en el período comprendido entre el 1 de enero del 2010 hasta el 21 de marzo del 2011, fecha de expedición de la mencionada Resolución;

Que, de acuerdo a lo señalado en el Art. 6 de dicha Resolución, la Superintendencia de Bancos y Seguros debe notificar a las instituciones bancarias involucradas con la lista de clientes perjudicados por transacciones y otros, devenientes del denominado "fraude informático";

Que, la Superintendencia de Bancos y Seguros y la Fiscalía General del Estado han advertido que las Instituciones del Sistema Financiero están desarrollando esfuerzos para evitar los problemas que los delitos informáticos pueden causar a los clientes del Sistema Bancario Nacional, así como su predisposición en el reconocimiento de las pérdidas ocasionadas en el patrimonio de sus usuarios por fraude informático;

Que, en la Resolución Interinstitucional No. 001-FGE-SBS-2011 no se estableció con claridad la forma en que los usuarios perjudicados debían manifestar su aceptación de los valores a ser devueltos por la banca;

Que, la tarea de la prevención de delitos informáticos es un ejercicio de todos los ciudadanos y de todas las instituciones públicas y privadas, procurando siempre el bienestar general y en consideración de que la actividad financiera es un servicio de orden público; y,

En mérito de las consideraciones señaladas, y en ejercicio de las facultades conferidas en la Constitución y en la Ley,

RESUELVEN:

EXPEDIR LA PRESENTE RESOLUCION ACLARATORIA A LA RESOLUCIÓN NO. 001-FGE-SBS-2011

Art. 1.- La Resolución Interinstitucional No. 001-FGE-SBS-2011 del 21 de marzo del 2011 se la expidió con el propósito de que las Instituciones Financieras Privadas atiendan y solucionen los reclamos y denuncias presentadas por sus clientes y usuarios, tanto en la Fiscalía General del Estado cuanto en la Superintendencia de Bancos y Seguros, dentro del período comprendido dese el 1 de enero del 2010 hasta el 21 de marzo del 2011.

Art. 2.- Los Clientes a los cuales las Instituciones Financieras devuelvan valores por perjuicios ocasionados por fraude informático, suscribirán con el Banco respectivo un Acta de conformidad, mediante la cual con la devolución y/o reintegro de valores se libera al banco pagador y a sus funcionarios, de cualquier otro nuevo reclamo sobre los mismos hechos materia de la denuncia. Estos reintegros no significan en modo alguno reconocimiento de responsabilidad de las instituciones financieras en los denominados delitos por fraude informático.

Art. 3.- Las Instituciones Financieras por los valores que reintegran voluntariamente tendrán el derecho de ejercer acciones legales en contra de quienes cometieron delitos de fraude informático, por lo cual recibirán de los usuarios perjudicados la colaboración necesaria.

Art. 4.- La Superintendencia de Bancos y Seguros y la Fiscalía General del Estado, en conjunto con las Instituciones del Sistema Financiero, colaborarán en las investigaciones sobre esta clase de delitos a fin de llevar a la justicia a los responsables de los mismos, en la forma prevista en la Ley, evitando así la impunidad.

Art. 5.- Los reintegros y los acuerdos ya firmados y procesados de manera voluntaria entre las Instituciones Financieras y los clientes perjudicados, no se verán afectados por lo dispuesto en el presente instrumento. Esta Resolución tampoco afectará a lo ya resuelto por la Superintendencia de Bancos sobre este tipo de reclamos.

Art. 6.- Si un usuario perjudicado no considerara conveniente aceptar los valores con aplicación de los porcentajes constantes en el Art. 4 de la Resolución No. 001-FGE-SBS-2011 del 21 de marzo del 2011, dispuestos a su favor, lo expresará, por escrito, a la Institución Financiera pertinente.

Art. 7.- La Superintendencia de Bancos expedirá normas que enfaticen la responsabilidad de los clientes por sus actos y omisiones en el manejo de sus claves secretas, y la obligación de utilizar sistemas informáticos seguros para sus transacciones electrónicas, en acuerdo con la educación financiera y la información entregada oportunamente por cada una de las instituciones del Sistema Financiero.

Art. 8.- La presente Resolución Aclaratoria entrará a regir a partir de la presente fecha, y de su efectivo control y seguimiento encárguese la Superintendencia de Bancos y Seguros, en su calidad de Organismo de Control de las Instituciones Financieras.

Dado y firmado en Quito, Distrito Metropolitano, a los veinte y cinco días del mes de abril del dos mil once.

Ab. Pedro Solines Chacón
SUPERINTENDENTE DE BANCOS Y SEGUROS

Dr. Washington Pesántez Muñoz
FISCAL GENERAL DEL ESTADO

CERTIFICAMOS que la Resolución que antecede, está suscrita por el señor abogado Pedro Solines Chacón, Superintendente de Bancos y Seguros y, por el señor doctor Washington Pesántez Muñoz, Fiscal General de Estado. Quito a, 25 de abril del dos mil once.

Abg. Luis Alberto Cabezas-Klaere
SECRETARIO GENERAL
SUPERINTENDENCIA DE BANCOS Y SEGUROS

Dr. Jorge Cevallos Dillon
SERETARIO GENERAL
FISCALIA GENERAL DEL ESTADO