



**LA RESPONSABILIDAD DE LAS ENTIDADES FINANCIERAS POR FRAUDES  
ELECTRÓNICOS**

JULIANA HERNÁNDEZ BOTERO

NÉSTOR RAÚL LONDOÑO SEPÚLVEDA

Doctor en Derecho

Director

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE MAGÍSTER EN  
DERECHO

MAESTRÍA EN DERECHO

ESCUELA DE DERECHO Y CIENCIAS POLÍTICAS

UNIVERSIDAD PONTIFICIA BOLIVARIANA

MEDELLÍN

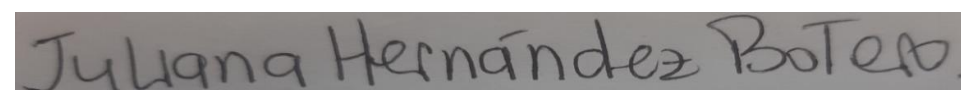
2020

**Medellín, 29 de julio de 2020**

**Juliana Hernández Botero.**

“Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad” Art. 82 Régimen Discente de Formación Avanzada.

Firma

Handwritten signature of Juliana Hernández Botero in black ink on a grey background.

---

Fecha: 29 de julio de 2020

Nombre del estudiante: Juliana Hernández Botero.

“Declaro que este trabajo de grado no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en esta o en cualquiera otra universidad”.

Nombre del director: Néstor Raúl Londoño Sepúlveda.

Nombre del jurado 1: José Fernando Ocampo Barrera.

Nombre del jurado 2: Hernán Vélez Vélez.

## Resumen

El presente artículo tiene por objeto presentar si es válido establecer, como lo señaló la Corte Suprema de Justicia en sentencia SC18614-2016, el régimen objetivo de responsabilidad (a pesar de aludir a la diligencia debida de los Bancos) en materia de fraude bancario por medios electrónicos, limitando los medios de defensa, excluyendo las causales de exoneración de ese régimen objetivo de responsabilidad, ignorando la naturaleza contractual de la relación, las órbitas de seguridad de cada parte y las regulaciones del comercio electrónico. Por ello, se propone una interpretación integral del ordenamiento jurídico para que en los análisis de este tipo de fraudes en el sistema financiero los aplicadores del derecho consideren la totalidad de los elementos que rodean la operación. Con base en lo anterior, se concluye que la responsabilidad por los fraudes electrónicos en materia bancaria por ser responsabilidad contractual debe resolverse de acuerdo con el cumplimiento de los deberes de diligencia de ambas partes, con criterios subjetivos y no con los criterios de la responsabilidad objetiva.

**Palabras clave:** Responsabilidad objetiva, responsabilidad subjetiva, fraudes electrónicos, informática, TIC, firma electrónica.

## Introducción

Con la tecnología de la información y las comunicaciones - TICs y en especial por la aparición del Internet y el nacimiento de las Apps<sup>1</sup>, es evidente que la forma de realizar las operaciones financieras ha cambiado. De la realización de dichas operaciones en forma presencial y en papel, donde existía un elemento de conocimiento personal del cliente en la agencia o sucursal bancaria donde se efectuaban, se ha pasado a la interacción electrónica. Las órdenes quirografarias que daba el titular de los derechos derivados de los contratos celebrados para las distintas operaciones y transacciones financieras han sido sustituidas por órdenes electrónicas y todos los días se reduce más esa presencia física del cliente, dando lugar a nuevas formas de realización de tales operaciones. Por ello, hoy se acuña una frase que resume lo anteriormente descrito: *“los que hoy están naciendo no entrarán jamás a un banco”* (Rincón, 2019).

Actualmente, en remplazo del conocimiento personal y directo del cliente al momento de realizar las transacciones bancarias, se ha pasado al concepto de “mecanismos de autenticación”, en otras palabras, para la realización de las transacciones financieras no es necesaria la presencia física de los clientes. Entre ellos cabe mencionar, las claves o números de identificación personal - NIPs, las claves dinámicas u OTP (*One Time Password* con segundo factor de autenticación) es decir, contraseñas de un solo uso que se remiten a los smartphones o al correo electrónico del cliente y hacen posible la transacción, los Token de autenticación y

---

<sup>1</sup> APP es una herramienta diseñada para desarrollar una función específica en una plataforma concreta: móvil, tablet, tv, pc, entre otros. El término se deriva de la palabra en inglés *application*, lo que significa Aplicación (App), se puede descargar o acceder a las aplicaciones desde un teléfono o desde algún otro aparato móvil – como por ejemplo una tablet o un reproductor MP3 (López Castañeda, 2016, p. 2).

los sistemas biométricos como lo son el reconocimiento de huellas dactilares, reconocimiento facial, reconocimiento de voz, del iris de los ojos, entre otros.

En tal sentido, el comercio electrónico hace posible las relaciones bajo otras ópticas y procesos. En esa transformación, el negocio financiero no se ha quedado atrás. Por eso, en la banca colombiana, desde 1996, se implementó la Sucursal Virtual Personas y en “1999 se empezó la sucursal virtual empresas, la cual propició el primer sistema de pagos por Internet en Colombia” (López, 2015).

Estos mecanismos de autenticación desarrollan el principio número 4 del documento emitido por el Comité de Supervisión Bancaria de Basilea, según el cual los bancos deben tomar medidas para autenticar la identidad y autorización de clientes cuando realiza transacciones por internet; que no es otra cosa que técnicas y procedimientos empleados para establecer la identidad del cliente y determinar el acceso legítimo a la cuenta, y que van a tener efectos en los casos de repudio y la consiguiente responsabilidad, situación que veremos posteriormente (Rincón, 2015).

Todo ello ha permitido la realización de millones de transacciones cada año en condiciones de seguridad y eficacia y con niveles bajos de repudio o fraude. Ello denota un alto nivel de seguridad, al estar complementados con las reglamentaciones de la ley de comercio electrónico, permiten predicar responsabilidades con mayor certeza y consecuentemente, pronunciamientos judiciales adecuadamente fundados.

Sin embargo, con la virtualidad se presentan riesgos sociales que han permeado la actividad financiera con la materialización en los fraudes informáticos como son el *phishing*, el *pharming*, *malware*, etc. Por lo anterior, es necesario analizar la responsabilidad en las

operaciones electrónicas de la banca, para determinar si se trata de un problema de responsabilidad objetiva, de actividades peligrosas o una responsabilidad basada en la culpa.

Por ello el presente trabajo versa sobre la responsabilidad de las Entidades Financieras por los fraudes electrónicos en las operaciones bancarias atendiendo todos los elementos que la integran y que fueron ignorados por la Corte Suprema de Justicia en sentencia SCI8614-2016. En tal sentido, nos planteamos el problema de si es válido establecer, como sentó el precedente la Corte Suprema de Justicia, responsabilidades objetivas en materia de fraude electrónico bancario ignorando la naturaleza contractual de la relación, las órbitas de seguridad de cada parte y las regulaciones del comercio electrónico.

Este objeto de investigación ha sido poco desarrollado en la literatura académica. A nivel cuantitativo, se cuenta con material importante en materia de responsabilidad bancaria, en general, que comprenden delimitación temporal desde el año 1999 hasta el 2019 (esto debido a que en Colombia, desde “1999 se empezó la sucursal virtual empresas, la cual propició el primer sistema de pagos por Internet en Colombia” (López, 2015) y se en ese mismo año se expidió la Ley 527 de 1999).

El desarrollo del presente estudio se realiza a partir del paradigma hermenéutico, en tanto presenta una propuesta de interpretación en los casos de responsabilidad bancaria en fraudes electrónicos. El método empleado fue el hermenéutico y se utilizó una técnica documental y jurisprudencial, porque se explican los eventos, las teorías, los elementos y conceptos que puedan solucionar las problemáticas que tienen los fraudes mediante sistemas electrónicos según la casuística. Como metodología se presenta una propuesta de interpretación en los casos de la responsabilidad bancaria en dichos fraudes, atendiendo los

elementos que integran las operaciones financieras y que fueron ignorados por la Corte Suprema de Justicia en Sentencia SCI8614-2016.

Este artículo contiene tres acápites, además de la introducción y la conclusión. La primera parte contiene la regulación en las operaciones mediante mecanismos electrónicos bancarios donde se presenta la actividad financiera; la relación contractual de los establecimientos bancarios con sus clientes, gozando estos de especial protección, por ser una relación asimétrica con posición de predominio de los bancos, y la normatividad base que se aplica de manera extensiva a la responsabilidad en las operaciones electrónicas bancarias. En la segunda, se explican los distintos aspectos de las operaciones electrónicas como lo son: los riesgos, las modalidades de fraude virtual, los efectos de la firma electrónica y las obligaciones de las partes. En la tercera, se cuestionan los aspectos expuestos sobre la responsabilidad bancaria en fraudes electrónicos en la decisión de la Corte Suprema en sentencia SCI8614-2016. Para lo cual se presentan: brevemente los hechos de la sentencia y las consideraciones de la Corte en sentencia SCI8614-2016; decisiones de la Superintendencia Financiera sobre este tipo de fraudes y finalmente se plantean críticas a la decisión de la Corte y la propuesta en torno al régimen de responsabilidad que propone este trabajo y que justificaría su implementación.



## **I. Regulación de las operaciones electrónicas bancarias.**

La actividad financiera es una actividad de interés público y de carácter profesional. Debido a la importancia de dicho sector en la economía, se presenta intervención estatal en el desarrollo de su actividad que tiene consagración constitucional. El artículo 335 de la Constitución Política establece que la actividad financiera requiere para su ejercicio autorización y va a ser regulada por la rama ejecutiva, precisamente por ser de interés público, lo cual conlleva la necesidad de preservar la estabilidad de la economía, los recursos de captación y promueve la democratización del crédito (Constitución Política de 1991, artículo 335). Lo cual ha sido reconocido por la jurisprudencia constitucional en Sentencia C-640 de 2010.

Con base en lo anterior, queda claro que las libertades económicas pueden ser limitadas y en este contexto la actividad financiera tiene restricciones enmarcadas no solo en la protección del interés público, sino también del consumidor financiero (Corte Constitucional, Sentencia C – 197 de 2012). En desarrollo de lo cual, en Colombia existen diversas normas que regulan la materia financiera, tales como el Estatuto Orgánico del Sistema Financiero, la Ley 1328 de 2009 Estatuto del Consumidor Financiero, el Decreto 2555 de 2010, la Circular Básica Jurídica 029 de 2014 de la Superintendencia Financiera de Colombia, ente otras.

Se destaca la Circular Básica Jurídica en la parte I, título II, capítulo I, numeral 2, sobre canales, medios y seguridad, específicamente el numeral 2.3.4.9, el cual consagra los requisitos que deben cumplir las entidades que ofrezcan la realización de operaciones por Internet como:

implementar los algoritmos y protocolos necesarios para brindar una comunicación segura; promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus operaciones monetarias pueda ser capturada por terceros no autorizados durante cada sesión; implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces de su sitio web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS; contar con mecanismos para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código o archivos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa y ofrecer a sus clientes mecanismos fuertes de autenticación<sup>2</sup>.

De otro lado, como se trata de operaciones que desarrollan comerciantes del negocio financiero, existen las regulaciones propias de los diferentes contratos bancarios que se encuentran en el Código de Comercio y las leyes que complementan esa actividad como lo son la Ley 527 de 1999 y su Decreto reglamentario 2364 de 2012 que regula las firmas electrónicas. En este mismo sentido, también es aplicable la Ley 1480 de 2011 Estatuto del Consumidor<sup>3</sup>.

La relación contractual entre entidades financieras y sus clientes no solo se encuentra regulada constitucional y legalmente, sino que demanda el ejercicio de la autonomía de la voluntad de las partes contratantes, lo cual va a dar lugar a un conjunto de deberes y

- 
4. La autenticación electrónica permite validar a los usuarios por medios electrónicos, en relación con un mensaje de datos y provee los mecanismos necesarios para firmarlos electrónicamente, en los términos de la Ley 527 de 1999 (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, 2018, p. 10).
  5. Concepto 2013008465-008 del 8 de julio de 2013 de la Superintendencia Financiera establece que la Ley 1480 de 2011 se aplica a las relaciones de los consumidores financieros con las entidades de manera supletoria o residual en aquellos eventos en que la normativa especial no regule un determinado tema.

obligaciones para cada una de ellas, ante cuyo incumplimiento deben responder por los perjuicios que se generen. Así las cosas, cuando se presenten casos donde el cliente objete a la Entidad Financiera una o varias operaciones electrónicas estamos siempre en presencia de una responsabilidad de naturaleza contractual bancaria.

En la relación contractual entre los establecimientos bancarios y sus clientes se evidencia que es el consumidor la parte débil frente al Establecimiento bancario el cual ostenta posición de dominio que se manifiesta, entre otros, por la contratación adhesiva (Gersovich, 2011, citado en Padilla y Zafra, 2017, p. 387). En tal sentido, al Banco le es aplicable una responsabilidad profesional, por ser una relación contractual de especial naturaleza, la legislación impone a las entidades financieras una conducta especialmente diligente (Padilla y Zafra, 2017, p. 386).

*En ese sentido, al momento de determinar la debida diligencia de las entidades financieras en sus relaciones con los consumidores financieros, es preciso señalar que aquellas son profesionales y que se encuentran frente a estos en una posición de asimetría contractual (Padilla y Zafra, 2017, p. 387).*

Lo cual implica que la diligencia que debe exigírseles a dichas entidades en el cumplimiento de sus obligaciones frente al ordenante o beneficiario ha de ser más estricta. El parámetro de conducta debe ser el comportamiento que llevaría a cabo una entidad financiera como profesional en el cumplimiento de sus obligaciones (Padilla y Zafra, 2017, p. 387).

En relación con lo anterior, en Colombia, existe el régimen general de protección a los consumidores, esto es, de la Ley 1480 de 2011 y un régimen especial de protección al consumidor financiero, consagrado en la Ley 1328 de 2009. Lo anterior significa que, en

Colombia, coexisten dos regímenes de protección al consumidor, se complementan para el equilibrio contractual en relaciones asimétricas. En efecto, la Ley 1480 de 2011 se aplica para las relaciones entre los establecimientos y el consumidor financieros en los casos no previstos en la Ley 1328 de 2009.

En tal sentido, a las Entidades Financieras se les exige el cumplimiento del principio de debida diligencia, para que las relaciones entre las entidades vigiladas y los consumidores financieros se desarrollen de forma que se propenda por la satisfacción de las necesidades del primero de acuerdo con la oferta, compromiso y obligaciones acordadas. *“Las entidades vigiladas deberán observar las instrucciones que imparta la Superintendencia Financiera de Colombia en materia de seguridad y calidad en los distintos canales de distribución de servicios financieros”* (Ley 1328 de 2009, artículo 3, literal a).

El marco regulatorio de responsabilidad en las operaciones virtuales bancarias ha sido objeto de creación por parte de la Jurisprudencia Colombiana, basada en los casos y normas del Código de Comercio (artículos 732 y 1391) sobre responsabilidad bancaria frente al pago de cheques adulterados o falsificados. Ello obedece a que tradicionalmente, los casos que se han presentado en temas de responsabilidad sobre operaciones bancarias corresponden a los casos de la responsabilidad de los establecimientos bancarios por el pago de cheques falsos o alterados, en cuyos casos se ha aplicado la responsabilidad objetiva.

En estricto sentido, este tema por el pago de cheques falsos o alterados no es el objeto de desarrollo en el presente artículo; sin embargo y teniendo en cuenta que la sentencia SCI8614-2016 objeto de cuestión, se basa en ello para hacer extensiva la aplicación de la responsabilidad objetiva a los establecimientos bancarios por fraudes electrónicos, resulta

pertinente abordar el tema, en tanto que es el fundamento que presenta una marcada influencia hacia la objetivación de la responsabilidad en los casos por fraudes electrónicos, desconociendo los cambios tecnológicos y por ende, dejando de lado importantes elementos, que deberían ser considerados.

La responsabilidad de los establecimientos bancarios por el pago de cheques falsos o alterados se encuentra regulada en el Código de Comercio. Los artículos 732 y 1391 consagran la responsabilidad bancaria en los casos de que el Banco efectúe el pago de cheques falsos o alterados que no han sido extraviados por parte del girador. Si no hubo culpa del cuentahabiente, el Banco responde, aunque haya existido culpa de su parte. El artículo 733 consagra la responsabilidad del cliente por haber perdido o extraviado los formularios de chequeras sin dar aviso oportuno al Banco.

Tomando como fundamento los enunciados normativos del Código de Comercio, se encuentra que la actual jurisprudencia Colombiana de la Corte Suprema de Justicia, atribuyéndole alcance y contenido a dicha normatividad (artículos 732 y 1391), adopta la posición de aplicar régimen objetivo de responsabilidad basada en el riesgo, señalando que cuando se presenta el pago de cheque falso la responsabilidad alcanza los riesgos: creado, beneficio y profesional, lo cual se explica en la segunda parte del artículo.

Recientemente, la jurisprudencia de la Corte Suprema de Justicia, en un caso de responsabilidad bancaria por cheques, expresa que por ser riesgosa la actividad financiera, existe presunción de culpa, así: *“La profesión bancaria envuelve una actividad riesgosa, motivo por el cual a quienes la ejercen se les exige la diligencia y cuidado necesarios para este tipo de actividades, lo que genera una presunción de culpa en su contra”*. (Corte Suprema de Justicia, 2019).

## **2. Efectos de la firma electrónica, riesgos y modalidades de fraude bancario electrónico.**

Para aproximarnos a los efectos y responsabilidades derivadas de las operaciones financieras electrónicas que hoy se hacen posibles con las TICs, es necesario comprender los aspectos legales del comercio electrónico y sus principios. En efecto, uno de sus principios pilares es el de Equivalencia Funcional de los Actos Electrónicos ya que es el fundamento de la interacción humana por medios electrónicos. Según este principio *“la función jurídica que cumple la instrumentación escrita y autógrafa respecto de todo acto jurídico, o su expresión oral, la cumple de igual forma la instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, extensión, alcance y finalidad del acto así instrumentado”* (Rincón, 2015, p.83). El principio está contenido en el artículo 6 de la Ley 527 de 1999 y la Corte Constitucional, al declarar la exequibilidad de la norma, señala que los mensajes de datos deben recibir el mismo tratamiento de los documentos escritos en papel, en otras palabras, las declaraciones de voluntad que se contienen en mensajes de datos tienen el mismo efecto que las contenidas en medios escritos.

El artículo citado fue reglamentado mediante el Decreto 2364 de 2012. Con este el Gobierno Nacional buscó impulsar el desarrollo del comercio electrónico, debido a que internacionalmente se ha recomendado promover enfoques apropiados para el reconocimiento legal de medios de identificación electrónica flexible y tecnológicamente neutras, que se adecúen a las necesidades de la sociedad y a las prácticas en entornos electrónicos.

El artículo 1 de dicho decreto define la firma electrónica como *“[m]étodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una*

*persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.”* De tal manera que resulta de vital importancia para predicar las responsabilidades en materia de fraudes virtuales, pues establece unas condiciones que el operador jurídico debe tener en cuenta, al lado de las cláusulas de los contratos bancarios que se celebran con el uso de medios electrónicos, cuestión que trataremos más adelante.

Como en toda actividad, la banca electrónica no está exenta de riesgos. Los riesgos en los contratos bancarios son de tres (3) clases: riesgos en la operación, riesgos de reputación y riesgos legales (Rodríguez citado en Rincón, 2015, 262).

El riesgo de operación se elimina, mitiga o controla mediante el uso actualizado de sistemas de *firewalls*<sup>4</sup>, dotando a las terminales, equipos de cómputo y redes locales de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones, protegiendo las claves de acceso a los sistemas de información. Estos cuidados impedirán que terceros no autorizados accedan en forma ilícita a los fondos o cuentas de los consumidores financieros o que mediante virus informáticos afecten directamente el sistema o la red del banco.

Ahora bien, dentro de los riesgos de la operación podemos mencionar los riesgos de suplantación, por lo que se hace necesario que se asegure que se está contratando o ejecutando una transacción con el destinatario deseado. El riesgo de alteración, que hace imperativo que los mensajes de datos que se generen envíen o reciban no son objeto de

---

<sup>4</sup> El firewall ofrece un punto donde la seguridad puede ser monitorizada y si aparece alguna actividad sospechosa, éste generará una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos. Esto es muy importante de cara a que el administrador audite y lleve un registro del tráfico significativo a través del firewall. También es importante que el administrador de la red responda a las alarmas y examine regularmente los registros de base (Pérez-Roca & Pereira Suárez, 2007, p. 4).

ninguna alteración o mutación. Los riesgos de ausencia de confidencialidad, que hacen necesario que se tenga un sistema con las especificaciones técnicas que aseguren que los mensajes de datos solo pueden ser conocidos por las partes o sujetos intervinientes.

En Colombia, la Superintendencia Financiera a través de la Circular Básica Jurídica señala unos requerimientos mínimos de seguridad y calidad para la realización de operaciones y brindar seguridad transaccional, dentro de los cuales podemos destacar las siguientes obligaciones de las entidades financieras: ofrecer los mecanismos necesarios para que los clientes tengan la posibilidad de personalizar las condiciones bajo las cuales realicen operaciones monetarias por los diferentes canales, siempre y cuando éstos lo permitan. En estos eventos se puede permitir que el cliente inscriba las cuentas a las cuales realizará transferencias, registre las direcciones IP fijas<sup>5</sup> y el o los números de telefonía móvil desde los cuales operará.

*Establecer procedimientos para el bloqueo de canales o de instrumentos para la realización de operaciones, cuando existen situaciones o hechos que lo ameriten o después de intentos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos (...)*

*Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes y definir procedimientos para la confirmación oportuna de las operaciones monetarias que no correspondan a sus hábitos (Superintendencia Financiera, Circular Básica Jurídica 2014).*

---

<sup>5</sup> La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos computadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos computadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique) (Universidad Técnica Federico Santa María, 2005, p. 3).



Bajo el riesgo reputacional, se incluirán las pérdidas sufridas por la entidad financiera cuyos sistemas no estén adecuadamente protegidos menoscabando la confianza general de los clientes. Por la naturaleza estratégica del sector, conforme a lo manifestado en la sección anterior, en la Circular Básica Jurídica se ha establecido la obligación de que las entidades financieras deben contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad y en las diferentes etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje, y en especial medidas de seguridad y de protección de la información.

Por otra parte, el concepto de riesgo legal está vinculado al análisis de las reglamentaciones de las operaciones electrónicas y los problemas de interpretación normativa en cuanto a los alcances de los derechos y obligaciones de los consumidores financieros que acceden a la contratación virtual. Por ello es que es necesario abordar el concepto de riesgo dentro de la responsabilidad civil, pues este es el elemento que imprime un carácter objetivo al análisis del régimen de responsabilidad.

La doctrina ha definido el riesgo como:

*[L]a contingencia de un daño; como la posibilidad o potencialidad de concreción de un daño. La idea de riesgo, con su introducción en la órbita del análisis de la responsabilidad, pretendió reemplazar la culpa como su elemento estructural principal. Esta subrogación implica un enfrentamiento con el principio según el cual no hay responsabilidad sin culpa probada, lo cual tiene como consecuencia que se le otorga una gran importancia al elemento del daño y no ya al de la culpa. Al reemplazar la categoría de culpa por la de riesgo, como base estructural de la responsabilidad, se*

*introduce un régimen de responsabilidad objetiva, en tanto se dejan de lado las consideraciones volitivas o internas de quien ha causado el daño (Sarmiento García, 1978, p. 128).*

En materia de responsabilidad civil, la jurisprudencia ha reconocido las siguientes teorías de riesgo: riesgo provecho, riesgo creado, riesgo profesional (Corte Suprema de Justicia, 2009). Lo cual, en materia de gestión de riesgos, da pie para afirmar que las entidades financieras tienen que cumplir una serie de obligaciones para evitar que estos se materialicen de tal manera que posibilite la realización de millones de transacciones en condiciones de seguridad y eficacia.

Lamentablemente no es posible predicar lo mismo del consumidor financiero, el cual es confiado y muchas veces imprudente y negligente en la gestión y prevención de los riesgos que se encuentran en su esfera de protección y cuidado motivado por la falta de educación financiera, asimetrías en la información, falta de cultura, entre otras<sup>6</sup>. En efecto, es usual que los clientes consumidores financieros compartan las claves con personas que le son cercanas multiplicando el riesgo, que no guarden con celo su información financiera sensible, que no custodien adecuadamente los *token* para realizar operaciones, no tener los mecanismos de protección en equipos computacionales o *smartphones* y que abran, descarguen y sigan instrucciones falsas de correos sospechosos que anuncian premios, eventos, necesidades de información, etc. para ser después objeto de saqueo de sus cuentas. Todas estas son circunstancias y hechos que estarán violado las normas y obligaciones contractualmente

---

<sup>6</sup> Actualmente en el tema de ciberseguridad se afirma “[p]eople are cyber security’s weakest link”, no obstante esto ha sido objeto de una enorme polémica, debido a que el factor humano no debería ser la excusa para un sistema débil de seguridad informática, usualmente las prácticas inseguras son señal de un problema sistémico (Oz Alashe, 2019).

asumidas por el consumidor y que de presentarse un fraude deben ser evaluadas por el operador jurídico al atribuir la responsabilidad.

Entre las principales modalidades de fraude virtual podemos mencionar los siguientes: el *Phishing*<sup>7</sup>, el *Pharming*<sup>8</sup>, el *Malware*<sup>9</sup>, entre otros (Ustariz, 2019, pp.122-138). Sin embargo, para efectos del presente artículo, se expondrá, más adelante, un caso sobre la modalidad *Phishing* que se presenta en la sentencia SC 18614-2016, objeto de cuestionamiento en el presente trabajo.

Todas estas situaciones, modalidades y riesgos nos permiten afirmar que en materia de sistemas para realizar operaciones electrónicas existirán siempre dos órbitas de custodia y protección: una, la del banco en relación con la protección de sus sistemas operativos y de información que deberán cumplir con la normativa que en Colombia está a cargo de la Superintendencia Financiera y, otra, la del consumidor financiero relacionada con el medio en el cual efectúan las transacciones y que bajo las exigencias de la vida en la actualidad, debe tomar conciencia y adoptar conductas de autoprotección.

---

<sup>7</sup> El *Phishing* es una modalidad de fraude que consiste en que el delincuente (*Phisher*) obtiene información del consumidor financiero en forma no autorizada mediante la utilización de correos electrónicos que buscan es “pescar” u obtener información sensible del cliente como contraseñas, identificación y cualquier otra información personal para luego con dicha información acceder a la entidad financiera y autenticarse como el cliente. Una de las modalidades más usadas es la de enviar el correo con la intención de que el cliente suministre la información que es redirigida a un sitio impostor para posteriormente efectuar el fraude.

<sup>8</sup> El *Pharming* es una modalidad de fraude que consiste en direccionar a la víctima a un servidor impostor para que allí las víctimas revelen su información. En esta modalidad aunque la dirección del dominio que el cliente ingresa en su computadora es la de la entidad financiera un archivo de host hace que en realidad se dirija a un sitio Web impostor.

<sup>9</sup> El *Malware* es una modalidad consistente en que se instala en el equipo un dispositivo o software malicioso en forma disimulada y desapercibida de forma tal que el usuario no se percata de él y ese programa espía recolecta la información sensible y confidencial del cliente, permitiendo incluso alterar el host del equipo para la ejecución posterior de un *pharming* afectando a la víctima. Una de las modalidades de malware es la instalación de Troyanos que son programas que aparentan tener una utilidad o beneficio para el usuario pero que en realidad tienen una finalidad maliciosa.

En Colombia los consumidores financieros tienen la oportunidad de señalar condiciones y reglas para la utilización de sus productos financieros, por ejemplo, de los canales y topes habilitados por el banco para que los consumidores hagan operaciones financieras, estos tienen la facultad de bloquear algunos de esos canales y definir los límites de los montos de conformidad con sus hábitos de operación electrónica.

En efecto, la Superintendencia Financiera en la Circular Básica Jurídica establece como obligación de las entidades financieras: *“ofrecer los mecanismos necesarios para que los clientes tengan la posibilidad de personalizar las condiciones bajo las cuales realicen operaciones monetarias por los diferentes canales, siempre y cuando éstos lo permitan”*. En estos eventos se puede permitir que el cliente inscriba las cuentas a las cuales realizará transferencias, registre las direcciones IP fijas y el o los números de telefonía móvil desde los cuales operará.

Todo este cambio en la manera de acceder a los servicios bancarios y las condiciones que rodean tales transacciones hacen necesario que el tema de la responsabilidad tenga que ser abordado con nuevas ópticas que analicen todas las facetas los sujetos intervinientes ya que predicar responsabilidades en forma genérica y con base en teorías surgidas bajo prácticas diferentes, resulta por demás impreciso y puede dar lugar a eventos de auto-fraude, injusticias, riesgos sistémicos, entre otros.

### **3. Análisis de la responsabilidad bancaria en los fraudes electrónicos desde la jurisprudencia.**

Como ya se afirmó, la Corte Suprema de Justicia en sentencia SC 18614-2016 decidió un caso de fraude electrónico, la cual ha sido la base de decisiones posteriores tanto de jueces como de la Superintendencia Financiera para la atribución de la responsabilidad en casos análogos. A continuación, se expondrán los hechos relevantes que se presentan en el caso que dio lugar a la polémica decisión.

En la sentencia en mención, la demandante es titular de una cuenta de ahorros. El Banco donde la titular adquirió el producto es el demandado y este habilitó como medio para que su cliente dispusiera de los recursos, la banca electrónica. La demandante manifiesta que accedió al sitio web del banco y su portal personal encontró que en su cuenta faltaba dinero. Ello fue producto de delito informático, *Phishing*. La demandante afirmó que actuó con diligencia y que el banco no le brindó educación financiera para evitar defraudaciones mediante delitos informáticos, ni implementó medidas mínimas de seguridad.

La Corte no casó la sentencia y declaró la responsabilidad civil de la Entidad Bancaria por considerar que el Banco incumplió con sus deberes de “*actuar con grado especial de diligencia en el desarrollo de las operaciones comerciales que constituyen su objeto social*”<sup>10</sup>, de brindar educación financiera, como compartir recomendaciones de seguridad y porque el Banco “*no acreditó la culpa del cuentahabiente*”.

---

<sup>10</sup> “(...)sostuvo que las entidades financieras están obligadas a atender las cuentas de sus clientes en «operaciones de retiro y canjes requeridas (...) sea usando los medios electrónicos o similares disponibles y ofrecidos por la entidad, siempre, sin descuidar su diligencia y cuidado profesional», lo que se acompasa con el deber de «actuar con grado especial de diligencia en el desarrollo de las operaciones comerciales que constituyen su objeto social», pues se le exige la diligencia y cuidado de «un profesional que deriva provecho económico de un servicio en el que existe un interés público», como señalan los artículos 72 y 98 numeral 4° del Decreto 663 de 1993” (Corte Suprema de Justicia, 2016).

La Corte en su análisis, parte de tomar los contratos bancarios típicos que permiten la captación, tales como el contrato de cuenta corriente y el contrato de depósito de ahorros, aplicando extensivamente el régimen de responsabilidad de los artículos 732 y 1391 C.Co. relativos al pago de cheques falsos o adulterados, a la responsabilidad por fraudes bancarios, fundamentándose en el régimen del sector financiero como una actividad profesional, basada en la teoría del riesgo.

Asimismo, la Superintendencia Financiera en la delegatura de funciones jurisdiccionales, ha proferido sentencias en acciones de responsabilidad contractual bajo la órbita de la protección al consumidor, señalando que no basta con que la entidad vigilada acredite que cumplió con los requerimientos mínimos de seguridad y calidad a su cargo para exonerarse de responsabilidad, pues también debe acreditar la culpa o negligencia concurrente de su cliente, quien a su vez, debe observar las disposiciones contractuales y las recomendaciones de seguridad impartidas por las entidades, pues éstas constituyen buenas prácticas de protección propia y tienen por finalidad evitar que terceros no autorizados tengan acceso a la información requerida para acceder a los recursos depositados<sup>11</sup>.

Adicionalmente, la Superintendencia en los casos de responsabilidad por fraudes virtuales bancarios analiza el perfil transaccional<sup>12</sup> del consumidor señalando al respecto que

---

<sup>11</sup> “Prácticas como descargar archivos adjuntos a correos electrónicos de dudosa proveniencia, constituyen inobservancia a esas buenas prácticas de autoprotección e incrementan el riesgo de ser infectado con virus informáticos, que permiten acceder a la información confidencial requerida para transar a terceros ajenos a la relación contractual. En este caso, adicionalmente la entidad financiera demostró haber cumplido con las obligaciones de seguridad de las operaciones a su cargo, por lo que se denegaron las pretensiones de la demanda” (Superintendencia Financiera, 2019).

<sup>12</sup> “Fraude Electrónico -Canal de Internet -Phishing - Transferencias a otras cuentas – Desatención recomendaciones de seguridad - Perfil transaccional. En el caso particular, se acreditó que en los términos y condiciones para la utilización del portal empresarial de Internet, estaba a cargo del consumidor, mantener los equipos utilizados para transar, libre de virus informáticos y con instalación de antivirus, no obstante, del análisis efectuado al computador del consumidor, se determinó que el mismo no cumplía con tales exigencias, lo que permitió que fuera infectado con malware malicioso, con lo que se acreditó que el consumidor, incumplió sus obligaciones contractuales y facilitó con ello el conocimiento por parte de terceros

*Ante la negación indefinida del cliente de no haber realizado operaciones por internet con cargo a los recursos depositados en su cuenta de ahorros, la entidad demandada debe probar la negligencia o culpa del consumidor financiero en el manejo de sus elementos e información requerida para transar y que existió inobservancia de las medidas de seguridad que debe tener en el uso del canal virtual, pues en caso contrario, se le considerará a la entidad financiera (Superintendencia Financiera, 2017).*

Para predicar responsabilidades por la materialización de riesgos de cualquier actividad humana, es necesario considerar todos los elementos que integran los hechos generadores de la misma, para hacer el juicio de imputación a un sujeto. La forma de vida actual con el uso de los dispositivos electrónicos, demanda comprender los contextos en los cuales se realizan los negocios y operaciones, teniendo en cuenta las condiciones que el comercio electrónico impone en las relaciones con los consumidores. Por lo tanto, las teorías que anteriormente señalaban una u otra consecuencia deben ser revaluadas con los nuevos elementos que la integran.

En este sentido, es importante traer a colación la postura del Dr. Tamayo quien señala que, erróneamente *“la jurisprudencia nacional, seguida, a menudo, por los autores, consideran que en materia financiera todas las obligaciones contractuales del banco son de resultado dizque porque la actividad financiera y bancaria es riesgosa o peligrosa”* (Tamayo, 2019). Como se mencionó inicialmente, en Colombia no hay regulación sustancial respecto a los fraudes en operaciones bancarias electrónicas, por lo que la jurisprudencia ha pasado a pronunciarse al respecto. La

---

*de la información transaccional, dado que el malware permitió manipular la información de las operaciones”* (Superintendencia Financiera, 2018).

postura de la Corte Suprema de Justicia en la sentencia en cuestión presenta consideraciones incoherentes.

La decisión de la Corte Suprema de Justicia, usando los lineamientos de la responsabilidad derivada de cheques falsos constituye para algunos juristas y funcionarios judiciales la base fundamental para definir el tratamiento de los fraudes electrónicos. Ejemplo de ello es la Sentencia del Tribunal Administrativo de Boyacá, con Magistrado Ponente Óscar Alfonso Granados Naranjo, proceso 2008-0369, en el cual se decidió un caso de *pharming* contra el Banco de Bogotá y que basó su decisión en la Sentencia cuestionada de la Corte. Por lo cual es indispensable analizar sus falencias.

Así, las normas relativas a los vacíos jurídicos (art. 8, Ley 153 de 1887) conducen a que, en este caso, ante la falta de norma sustancial que rijan la materia, debe aplicarse por analogía la regulación y el régimen de responsabilidad relativo a otro tipo de fraudes, como por ejemplo el de pago de cheques falsos o adulterados. Como ya se ha indicado, en los artículos 732 y 1391 C.Co se imputa objetivamente el perjuicio al banco. Ello ignora que, con el pasar del tiempo y con los desarrollos tecnológicos como ya se ha señalado, la forma de operar las transacciones financieras ha cambiado, y por consiguiente, las modalidades de fraude en las mismas. Adicionalmente, la Corte se olvida de aplicar la responsabilidad con culpa consagrada en el artículo 733 del C.Co., el cual se considera que es realmente el caso análogo aplicable al fraude electrónico, pues al tratarse del pago del título falsificado, antecedido de su extravío en poder del cuentahabiente, es éste quien asume las consecuencias de la falta de cuidado en la custodia de los formatos o formularios de cheques. De ahí que el hecho de su pérdida le es atribuible, y en esa medida le corresponde asumir los efectos del pago que haga el Banco, salvo que



oportunamente le hubiere avisado a la entidad sobre la pérdida o que la falsedad o adulteración fuera evidente o notoria.

Así las cosas, es al cliente a quién le corresponde la obligación de custodia de los formularios de cheques que son los medios para la disposición de los recursos monetarios, obligación que desde el punto de vista fáctico sería imposible asumir por parte del Banco. Por ello, es al cliente a quien le corresponde demostrar la notoriedad de la falsificación o alteración, o que, en caso de que la falsedad no sea evidente, le avisó a la entidad tal hecho antes de que procediera al pago.

En los fraudes electrónicos el medio para la transacción no es el cheque, sino los mecanismos de autenticación, aplicar análogamente esa situación hace que el régimen de responsabilidad se traslade del banco al cliente a menos que la falsedad sea notoria, que bajo las condiciones actuales, ello sería equivalente a que el Banco incurra en fallas en el análisis de las condiciones en las cuales se realizaron las transacciones que se objetan, vale decir, si existen por parte del Banco situaciones notorias que en su carácter de profesional debe detectar como es el hecho de que las operaciones se generaron de direcciones IP diferentes, no se adecuaron al perfil transaccional del cliente, se hicieron en un canal no autorizado por este, superaron el tope establecido, etc.

En otras palabras, el supuesto planteado en el artículo 733 del C.Co se considera el más análogo al caso de fraude electrónico por delitos informáticos como el *phishing* expuesto en la Sentencia objeto de cuestión, debido a que en ambos casos se presenta: en primer lugar, la pérdida del medio (concretamente, en dicha disposición, el cheque o talonario y en los casos de fraudes virtuales equivaldrían a los mecanismos de autenticación como claves) por parte del

titular de la cuenta o de la persona autorizada por el titular para disponer de los recursos depositados en la cuenta de depósitos, sin dar aviso oportuno al Banco de tal hecho; y en segundo lugar, el supuesto de que la alteración o falsificación fueren notorias que en el caso de los cheques se presenta cuando la firma sea notoriamente diferente a la registrada por el girador y en los fraudes electrónicos corresponde específicamente a transacciones por fuera del perfil transaccional, de canales y de topes señalados por el cliente. En este sentido, la Corte en la sentencia cuestionada no acogió el texto legal que en el hecho positivamente regulado presenta la mayor analogía.

Por lo anterior, se está en presencia de situaciones que requieren un análisis bajo la estructura de la responsabilidad por culpa o aquiliana empleando el verdadero texto legal al hecho análogo. Sin embargo, las atribuciones patrimoniales de responsabilidad en los fraudes electrónicos bancarios presentadas en la sentencia SCI8614-2016, reflejan la tendencia alrededor de considerar la profesión financiera una actividad de riesgo, aplicando extensivamente a todos los casos de responsabilidad bancaria el régimen de responsabilidad objetivo.

Por otra parte, la Corte no tuvo en cuenta la existencia del contrato bancario, que para el caso concreto correspondía al “reglamento de convenios para la prestación de servicios bancarios”<sup>13</sup> que regía la relación en medio de la cual se presenta un supuesto fraude electrónico, ignorando las obligaciones contractuales de diligencia y cuidado de cada una de las partes (del cuentahabiente tener suficiente diligencia y cuidado con sus claves y entrar directamente al sitio web del Banco, y de la Entidad Bancaria adoptar las medidas de seguridad

---

<sup>13</sup> “(...) reglamento de convenios para la prestación de servicios bancarios aceptado por la depositante [Folios 141-145, c. 1].” (Corte Suprema de Justicia, 2016).

como compra de servidor, software y renovación de servicios de seguridad informática para salvaguardar la información de los clientes cuando ingresen en el portal virtual), es decir, desconoció la Corte la autonomía de la voluntad de las partes, el alcance jurídico de las claves electrónicas y los parámetros de seguridad que cada una debe cumplir acorde con lo pactado. En consecuencia, la Corte ignoró las condiciones de la responsabilidad contractual, pues con la banca electrónica no solo se beneficia el establecimiento bancario sino también el consumidor, por lo que sería aplicable el artículo 1604 C.C.

En tal sentido, la Corte desconoce que el riesgo tecnológico es un riesgo compartido y conocido entre las partes, por lo tanto, la responsabilidad debe ser basada en la culpa, atendiendo además a que el beneficio es para ambas partes, como ya se indicó. Para el cliente los costos para transar son menores, mayor seguridad personal, evitar desplazamientos, optimiza el tiempo y permite realizar operaciones en cualquier parte del mundo, entre otros.

En consecuencia de lo anterior, en la sentencia en cuestión, se encuentran inconsistencias como: aplicar el régimen de responsabilidad objetiva, pero mencionando la diligencia debida de los bancos; desconocer el contrato para la asignación de riesgos y las obligaciones asumidas; impedir al Banco alegar la causa extraña como causal de exoneración e imponer, como si fuera tarifa legal, como única prueba la culpa del cuentahabiente con un supuesto normativo que no es el apropiado, limitando los medios de defensa.

Es importante que en el análisis de responsabilidad en fraudes electrónicos se considere la importancia de la conducta de la víctima para la determinación de la reparación de los daños que ésta ha sufrido, pues desde el derecho romano se aplicaba en forma drástica la regla, atribuida a Pomponio, según la cual *“quod si quis ex culpa sua damnun sentit, non intellegitur*

*damnum sentire*”, es decir, que el daño que una persona sufre por su culpa se entiende como si no lo hubiera padecido (Jaramillo Jaramillo, 2013, p. 97).

Hoy en día la virtualidad empuja a los sujetos a actuar utilizando los elementos tecnológicos que se ponen a su disposición. La accesibilidad del cliente al banco para realizar una transacción financiera se produce mediante la utilización de un mecanismo de autenticación convenido entre las partes, que está en poder y bajo custodia del consumidor financiero y que en principio lo desconoce el Banco. El consumidor tiene obligaciones expresas de custodia y buen manejo de su firma electrónica de conformidad con la Ley 527 y el Decreto 2364 de 2012. En todo este escenario planteado no parece posible predicar responsabilidad objetiva, por tanto, se considera que la Corte en su decisión ignoró elementos indispensables para predicar la responsabilidad dejando de lado los principios de integralidad y justicia. En consecuencia, si existen normas que le dan efectos a las firmas electrónicas, hay regulaciones sobre la seguridad que deben tener las partes en este tipo de transacciones, textos legales que pueden utilizarse por analogía y se celebran contratos que regulan los aspectos inherentes a estas operaciones, resulta un despropósito acudir a la responsabilidad objetiva.

La Corte Suprema ha afirmado que, para exonerarse de responsabilidad, los bancos deben demostrar un incumplimiento del cliente y además acreditar el cumplimiento de obligaciones tales como: i) elaborar un perfil de costumbres transaccionales para cada cliente, que consiste en un análisis de las transacciones habituales realizadas por el cliente teniendo en cuenta los días, montos, destinatarios e incluso dirección IP desde la cual realiza habitualmente dichas operaciones, entre otros; ii) proceder con el bloqueo preventivo de la cuenta en caso de

advertir operaciones que no se adecuen al perfil transaccional del cliente. No basta con la notificación al cliente de las operaciones inusuales.

Finalmente, la sentencia objeto de discusión refleja una confusión, mezclando los regímenes de responsabilidad, en tanto que presenta incongruencias tales como, optar por la aplicación acomodada a un régimen de responsabilidad objetiva en los fraudes electrónicos con fundamento en el riesgo profesional y al mismo tiempo valora el cuidado y la diligencia con que deben obrar los bancos. Como se expresó anteriormente, ignorar las responsabilidades legales y contractuales y los deberes de diligencia de las partes para predicar después responsabilidades objetivas es absurdo porque ante un verdadero régimen de responsabilidad objetiva, no es tema de estudio ni de análisis, circunstancia que genera confusión.

*Por lo tanto, la responsabilidad objetiva por riesgo en la actividad financiera es válida solo en materia extracontractual, si con ella se pone en riesgo el patrimonio de los terceros ajenos a un contrato; como cuando una entidad financiera, alegando la libertad de mercado, desata una peligrosa especulación accionaria que arruina a todo el universo inversionista. Pero frente a sus acreedores contractuales, la responsabilidad será objetiva o culposa dependiendo únicamente del tipo de obligaciones contraídas (...)*

*El argumento del riesgo social que esgrime la Corte es un juego de palabras, pues si así fuera, la responsabilidad de los médicos siempre sería objetiva, pues nada hay más riesgoso para la sociedad que el ejercicio de la medicina (...)*

*Acudir a la responsabilidad por actividades peligrosas o riesgosas a todos los contratos financieros significa la aplicación de la responsabilidad extracontractual por actividades*

*peligrosas, consagrada en el artículo 2356 del Código Civil, a la responsabilidad contractual financiera (Tamayo, 2019).*

Por eso, en los eventos de fraude electrónico, se hace necesario plantear esquemas de responsabilidad que se derivan de las diferentes conductas de los agentes participantes y que no pueden, por diferentes circunstancias y análisis jurídicos, definirse bajo los criterios de responsabilidad objetiva ya que el mundo de hoy impone a los sujetos tomar medidas de autoprotección dado el ambiente en que se desarrollan y las diferentes modalidades de afectación. En efecto, las regulaciones de las entidades financieras hoy exigen unas condiciones de seguridad y el cumplimiento de mecanismos de autenticación fuertes adicional a operaciones de monitoreo. Estas regulaciones imponen a las entidades financieras ser diligentes y cumplir con una serie de condiciones que vislumbran responsabilidades en la medida que se satisfagan o no estos deberes. De otro lado, y en la medida de que el uso de los productos financieros por medios virtuales no hacen necesaria la presencia física del consumidor financiero, los elementos de identificación y de autenticación que permitirán acceder a ellos, requerirán del cumplimiento de unas obligaciones contractuales que garanticen privacidad, no solo de la información sensible, sino también del cuidado y diligencia en el uso de los medios habilitados para actuar en este escenario virtual. En este sentido, la ley de comercio electrónico y los decretos reglamentarios de la firma electrónica tienen unos efectos que no se pueden desconocer.

Por último, basarse en el artículo 732 y 1391 del C. de Co, cuando el supuesto fáctico se asemeja más a las circunstancias que se consagran en el artículo 733 del mismo estatuto mercantil, constituye un despropósito por lo que se hace necesario, replantear el tema considerando los elementos descritos.

## Conclusiones

En materia de responsabilidad por fraudes en operaciones bancarias electrónicas, se ha aplicado extensivamente la responsabilidad por el pago de cheques falsos o adulterados, ante la ausencia de norma sustancial que regule la materia. Ello implica que se presenta una tendencia generalizada de aplicación de régimen de responsabilidad objetiva, por el riesgo. Contradictoriamente, el aplicador del derecho valora la diligencia y cuidado de las entidades financieras, como si se tratara de un juicio basado en la responsabilidad con culpa.

Se considera que en estos casos lo que procede es realizar un análisis integral de todos los elementos jurídicos involucrados (contrato bancario, alcance jurídico de las claves electrónicas y digitales, las obligaciones de seguridad), además de tener en cuenta la justicia, la equidad y la reparación integral del daño. En consecuencia, se propone un mayor rigor en el análisis de la responsabilidad por fraudes en operaciones bancarias electrónicas, acudiendo a la aplicación de régimen subjetivo de responsabilidad, en tanto que se debe promover una reciprocidad de esfuerzos entre el banco y el cliente, por la naturaleza y condiciones de los mecanismos electrónicos, en aras de evitar la ocurrencia del daño.

En relación con lo anterior, es menester considerar que cuando se establecieron claramente la asunción de riesgos de acuerdo a las obligaciones diligencia, custodia y seguridad para cada parte y se presenta sustracción de dinero de una cuenta de depósito producto de un delito informático, la pérdida patrimonial debe ser asumida por quién incumplió tales obligaciones y si concurren las culpas de las partes, la pérdida patrimonial la asumirá cada una en proporción a la incidencia causal en el hecho pues sería absurdo aplicar la responsabilidad extracontractual por actividades riesgosas a la responsabilidad contractual financiera.

## Referencias

### Libros

Goodman, M. (Ariel). (2016). *Los Delitos Del Futuro*. Bogotá: Editorial Planeta.

Jaramillo, Carlos Ignacio. (2013). *Los Deberes de Evitar y Mitigar el Daño. Funciones de la Responsabilidad Civil en el siglo XXI y trascendencia de la prevención*. Bogotá: Editorial Temis.

Márquez, S. S. (2016). *Bitcoin, guía completa de la moneda del futuro*. Bogotá: Ediciones de la U.

Rincón, C. E. (2015). *Derecho del Comercio Electrónico y de Internet*. Bogotá: Legis.

Rodríguez, A. S. (2009). *Contratos Bancarios*. Bogotá: Legis.

Tamayo, J.J. (2007). *Tratado De Responsabilidad Civil*. Bogotá: Segunda Edición. Legis.

Tamayo, L. A. (2005) *La responsabilidad civil extracontractual y la contractual*. Bogotá: Ediciones Doctrina y Ley Ltda.

Ustariz, L.H. (2019) *Responsabilidad bancaria por fraude electrónico*. Bogotá. Editorial Ibañez.

### Artículos

Padilla Sánchez, Jorge Alberto y Zafra Sierra, Málory. (2017). Responsabilidad de los establecimientos bancarios por el pago de cheques falsos o alterados en Colombia. *Revista de derecho privado*.

Marusic. M.M. (2019). *LA TERCERA. Pulso*. Corte Suprema falla que los Bancos deben hacerse cargo de los fraudes informáticos. Recuperado de <https://www.latercera.com/pulso/noticia/corte-suprema-falla-los-bancos-deben-hacerse-cargo-los-fraudes-informaticos/570975/>



Tamayo, J.Javier. (2019). *Ámbito Jurídico*. La responsabilidad contractual bancaria no se basa en la teoría de las actividades peligrosas o riesgosas. Recuperado de <https://www.ambitojuridico.com/noticias/columnista-impreso/administrativo-y-contratacion/la-responsabilidad-contractual-bancaria>

Rodríguez Zárate, A. (2014) Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos. El riesgo provecho. El riesgo creado y el riesgo profesional. (Tesis de Maestría, Pontificia Universidad Javeriana, Bogotá, Colombia). Recuperada de <https://revistas.javeriana.edu.co/index.php/vnijuri/article/view/10176>

Pérez-Roca y Pereira Suárez. (2007) *Firewalls*. Recuperada de <http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/06%20-%20Firewalls%20%5Bupdated%5D.pdf>

Oz Alashe. (2019). *Are Humans Really “The Weakest Link” In The Cyber Security Chain?* Recuperada de <https://www.cbronline.com/opinion/are-humans-really>

Universidad Técnica Federico Santa María. (2005). *Introducción Ingeniería Informática*, p. 3. Recuperado de <https://www.inf.utfsm.cl/~contrera/IntroIngelInfo/apuntes/IPintroduccion.pdf>

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2018). *Manual de Condiciones Servicio de Autenticación Electrónica*, p. 10. Recuperado de [http://micrositios.mintic.gov.co/servicios\\_ciudadanos\\_digitales/autenticacion\\_electronica/3\\_1\\_manual\\_condiciones\\_servicio\\_autenticacion\\_electronica.pdf](http://micrositios.mintic.gov.co/servicios_ciudadanos_digitales/autenticacion_electronica/3_1_manual_condiciones_servicio_autenticacion_electronica.pdf)

**Conferencia:**

Rincón, E. (2019, 13 de junio). Aspectos Legales y jurídicos de BlockChain. Tendencias y Oportunidades. Evento realizado en Factoría Space, Medellín.

### **Normas:**

Tafur, González. Álvaro. (Vigesimaquinta Edición). (2007). Código Civil Anotado. Bogotá, D.C.:Leyer.

Colombia. LEY 153 (1887).

Leal, Pérez. Hildebrando. (Vigesimasexta Edición). (2010). Código de Comercio Anotado. Bogotá, D.C.:Leyer.

Colombia. Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia.

Colombia. Congreso de la República. LEY 527 (1999).

Colombia. Congreso de la República. LEY 1328 (2009).

Colombia. Congreso de la República. LEY 1480 (2011).

Colombia. Presidencia de la República. 2555 (2010).

Colombia. Presidencia de la República. Decreto 2364 (2012).

Colombia. Superintendencia Financiera. CIRCULAR 029 (2014).

### **Sentencias:**

Corte Suprema de Justicia. (2009). Bogotá. SC exp. 1100131030382001-01054-01.

Magistrado Ponente: William Namén Vargas.

Corte Suprema de Justicia. (2016). Bogotá. SC18614-2016. Magistrado Ponente: Ariel Salazar Ramírez.

Corte Suprema de Justicia. (2019). Bogotá. SCI697-2019. Magistrada Ponente: Margarita Cabello Blanco.

Corte Constitucional. (2010). Bogotá D.C. Sentencia C – Sentencia C-640 de 2010. Magistrado Ponente: Mauricio González Cuervo.

Corte Constitucional. (2012). Bogotá D.C. Sentencia C – Sentencia C-197 de 2012. Magistrado Ponente: Jorge Ignacio Pretelt Chaljub.

Tribunal Administrativo de Boyacá. (2018). Boyacá. Sala de decisión 5. Radicado. 2008-0369. Magistrado Ponente: Óscar Alfonso Granados Naranjo.

Superintendencia financiera Financiera. (2019). Bogotá. Delegatura Funciones Jurisdiccionales. Radicado 2018-1178. 2018070566.

Superintendencia Financiera. (2018). Bogotá. Delegatura Funciones Jurisdiccionales. Radicado 2017034137 2017-0528.

Superintendencia Financiera. (2017). Bogotá. Delegatura Funciones Jurisdiccionales. Radicado 2016118159 2016-2091