

Radicación	05001 40 03 018 2013 01299 01
Tipo de Proceso	Ordinario – Responsabilidad Civil Contractual
Demandante	Juan Felipe Yasser
Demandado	Banco AV Villas
Sentencia Nro.	019
Instancia	Segunda
Decisión	Confirma sentencia apelada.

**REPÚBLICA DE COLOMBIA
RAMA JUDICIAL DEL PODER PÚBLICO**



JUZGADO VEINTIDÓS CIVIL DEL CIRCUITO DE ORALIDAD

Medellín, Catorce (14) de diciembre de dos mil veintitrés (2023)

1. OBJETO DE LA DECISIÓN

Se procede a decidir el recurso de **APELACIÓN** interpuesto por el apoderado judicial que representa la parte demandante, en contra de lo resuelto en la sentencia proferida por el **JUZGADO VEINTINUEVE CIVIL MUNICIPAL ORALIDAD DE MEDELLÍN**, el 29 de noviembre de 2022, en el presente proceso Ordinario de Responsabilidad Civil Contractual, promovido por el señor **Juan Felipe Yasser**, en contra del señor **Banco AV Villas**.

2. ANTECEDENTES

2.1. LA DEMANDA

El 6 de noviembre de 2013, el señor **Juan Felipe Yasser**, por medio de apoderado judicial, presentó demanda ordinaria de responsabilidad civil contractual ante los Jueces Civiles Municipales de Medellín (Reparto), en contra del **Banco AV Villas**, quien describió como fundamentos fácticos que el día 15 de marzo de 2013 se dirigió a la sucursal del banco demandado, sede la América de esta ciudad para realizar un retiro, sin embargo, ello no fue posible por cuanto una funcionaria del Banco le explicó que la tarjeta se encontraba bloqueada por seguridad, dado que el día anterior se había detectado una transacción sospechosa por valor de \$1.000.000. El señor Yasser confirmó que él había realizado la transacción y que por consiguiente no era necesario proceder con el bloqueo de la tarjeta, sin embargo, como esa medida ya se había generado, le informó la asesora que después del mediodía del 15 de marzo de 2013 se reactivaría la tarjeta y se le informaría.

Refiere que a las 12:45 del día 15 de marzo de 2013, recibió una llamada del Call Center del Banco AV Villas, para preguntarle si se había efectuado un retiro con la tarjeta débito, a lo que contestó que no, porque el producto se hallaba bloqueado y estaba a la espera que le conformaran su reactivación; de nuevo se le indagó si había realizado una transacción por valor de

\$13.450.000, a lo que respondió nuevamente que no; luego le insiste que si autoriza dicha transacción, a lo que el señor Yasser manifiesta que no. Dado lo anterior, le fue sugerido por la asesora que se acercara lo más pronto posible a una oficina del Banco AV Villas.

Cuando se hallaba en camino a la sucursal, recibió una llamada de la señora “Leidy Lorena Vélez”, quien le informó sobre el desbloqueo de la tarjeta y él la puso al tanto de lo sucedido en la anterior llamada, y que se encontraba camino a la sucursal ubicada en el barrio la América. Una vez se halló en el sitio, se le indicó que el crédito rotativo había bajado a su cuenta de ahorros la suma de \$13.450.000, suma con la cual se hizo un pago por PSE por concepto de seguridad social, por un valor total de \$13.891.771. Por sugerencia de la funcionaria que brindó la información el señor Juan Felipe bloqueó su cuenta y las claves de todos los canales de comunicación.

Debido a esta circunstancia, refiere el demandante que el 19 de marzo de 2013, se dirigió a la Fiscalía a formular denuncia por el delito de hurto por medios tecnológicos y semejantes; además promovió una queja ante la sucursal del banco Av Villas del Barrio la América, con radicado N° 6067888, y, presentó un derecho de petición, ante la misma entidad bancaria, para que le fuera reintegrado el dinero.

A inicios del mes de abril de 2013, el Banco AV Villas dio respuesta a la petición N° 6067888. De acuerdo con su contenido, se le hizo saber que para la inscripción del servicio de banca Personal por internet fue necesario la digitación de datos personales tales como, número de identificación, número de producto a inscribir, clave secreta de tarjeta y número de tarjeta; y basado en esos datos, la transacción pedía la utilización de los elementos de seguridad, que en efecto fueron suministrados, en virtud de lo cual no es posible acceder al reintegro del dinero.

Relata que el día 05 de junio de 2013, agotó un nuevo derecho de petición ante el ente financiero, cuya reclamación fundamentó en la obligación de seguridad que tiene el Banco frente a transacciones fraudulentas por medios informativos, que se trata de un riesgo propio de la actividad que no tiene por qué sumir el cliente. En tal sentido reclamó suspender el pago de las cuotas mensuales, reintegrar el dinero pagado por concepto de la transacción fraudulenta e identificar el titular de la cuenta a la que se realizó la consignación.

El 26 de julio de 2013 recibió respuesta del Banco Av Villas, donde negó su responsabilidad frente a la transacción por haberse usado los elementos de seguridad exigidos; frente a la identificación de la cuenta a la que se realizó la transferencia por valor de \$13.891.771, sólo brindó el número de cuenta, no la identificación de su titular, que resulta indispensable para establecer el responsable del fraude.

Conforme a los anteriores hechos, enunció como **Pretensiones:** que se declare al Banco AV Villas civilmente responsable de los perjuicios patrimoniales y extrapatrimoniales por el fraude realizado por medios electrónicos sobre la cuenta de ahorros No. 52570818 cuyo titular es el señor Juan Felipe Yasser, a raíz de la transacción de fecha 15 de marzo de 2013, en la que trasladaron del crédito rotativo del demandante a la cuenta de ahorros indicada la suma de \$13.000.000, suma que al igual que otros \$891.771, fue transferida a otra cuenta bajo la denominación de COMPRA PSE SOI ACH, dado que la entidad demandada incumplió su obligación contractual de seguridad y diligencia, basada en la confianza pública que se deposita en la institución financiera.

Como consecuencia de esa declaración de responsabilidad, que se condene al banco Av Villas a pagar por concepto de perjuicios patrimoniales y extrapatrimoniales las sumas que se indican a continuación y las que resulten probadas en el proceso, y que deben ser debidamente indexadas.

Perjuicios patrimoniales:

A título de **daño emergente pasado:**

-Gastos de abogado para asesoría y elaboración de derecho de petición ante el banco \$800.000;
-El valor de la transferencia fraudulenta \$13.891.771;
-El valor de las cuotas mensuales e intereses generados como consecuencia de la transferencia fraudulenta y de la activación del crédito rotativo: marzo \$383.833, abril \$679.138, mayo \$1.331.021, junio \$663.254, julio \$650.078, agosto \$650.078, septiembre \$650.078. Para un total de \$5.007.324

A título de **daño emergente presente:**

La cuota del mes de octubre con sus intereses, que se calcula en la suma de \$650.000

A título de **daño emergente futuro:**

Las cuotas mensuales e intereses generados como consecuencia de la transferencia fraudulenta y la activación de crédito rotativo que se lleguen a causar, y se calculan en promedio en la suma de \$650.000 mensuales, por un periodo probable de dos años, para un total de \$15.600.000

Para un total de daño material estimado en \$35.949.095.

Perjuicios por alteración las condiciones normales de existencia, por su alteración en ocupaciones, hábitos o proyectos, pues dado los pagos mensuales que debe realizar por cada cuota, el demandante no puede asumir los gastos de manera normal, la suma equivalente a 25 SMLMV, esto es, \$14.737.500.

Perjuicios extrapatrimoniales

A título de **perjuicio moral** la suma equivalente a 25 SMLMV, esto es, \$14.737.500. Por el estrés y angustia generada por el hurto, situación de inseguridad frente al banco, que en su caso por ser comerciante es mucho más gravosa. Máxime que no tiene certeza si puede o no cubrir sus gastos familiares y si podrá o no realizar los proyectos que tenía a mediano y largo plazo.

2.2. CRÓNICA PROCESAL PRIMERA INSTANCIA

La demanda Ordinaria fue repartida al Juzgado Segundo Civil Municipal de Descongestión de Medellín, quien el 07 de febrero de 2014, inadmitió la demanda y concedió el término de ley para subsanar requisitos. Cumplidas las exigencias, en auto calendarado, 26 de febrero de 2014, se dispuso admitir la demanda de responsabilidad civil contractual formulada por **Juan Felipe Yasser** en contra del Banco AV Villas. Se dispuso adelantar el proceso por el trámite abreviado y surtir la notificación de la entidad demandada

Posteriormente, tras la solicitud que elevara el extremo demandante, mediante auto de fecha 28 de abril de 2014, se decretó la medida cautelar que consiste en la suspensión de las cuotas mensuales a cargo del señor Juan Felipe Yasser titular de la cuenta de ahorros Nro. 52510818 del Banco Av Villas.

De acuerdo con el acta fechada 04 de agosto de 2014, compareció a recibir notificación personal la apoderada judicial designada por el banco Av Villas para su representación, a quien se le concedió el término de 10 días para presentar contestación de demanda.

La contestación de demanda fue radicada el 20 de agosto de 2014, en la que se opone a las pretensiones y para sustentar su defensa formula los siguientes medios exceptivos:

Culpa de la víctima e incumplimiento de sus obligaciones contractuales. Los hechos que dan lugar a la reclamación surgen de un ilícito penal denominado hurto por medios electrónicos, que fue cometido por terceros ajenos al banco, que accedieron a la banca personal por internet con el usuario y clave secreta del demandante, de allí hicieron una transferencia que contó con todos los elementos de seguridad del demandante, pues se efectuó desde la banca personal por internet del cliente y con el usuario que tiene registrado desde el 7 de noviembre de 2006.

Refiere que al momento de la inscripción al servicio de Banca Personal por Internet el cliente debió suministrar los datos de número de identificación, número de producto a inscribir, clave secreta de la tarjeta y número de la tarjeta. El contrato de aceptación a este servicio suscrito por el cliente tiene indicado en sus políticas que el cliente es el único que debe conocer la clave y que acepta que no la dará a conocer a terceros, que es de su entrega responsabilidad la confidencialidad de la misma. Bajo ese supuesto indica que la comisión del delito responde a la negligencia y descuido del cliente. El sistema de consulta interna arrojó la siguiente información: la transacción fue realizada desde el usuario jyasser10, asignado por el cliente al momento de la suscripción del servicio; el usuario del cliente reporta ingresos desde 7 direcciones IP diferentes, lo constituye un hábito transaccional en internet; se hizo una solicitud de clave temporal desde el usuario del cliente, que se remitió a su correo electrónico registrado desde el 7 de septiembre de 2009; y desde el usuario del cliente se registraron preguntas de seguridad el día 15 de marzo de 2013 a las 11:42:02 a.m.

Ilícito penal. En la medida en que se sustrajo un dinero a través de medios electrónicos, que había sido suministrado por el Banco al cliente. Ese ilícito configura una acción penal y civil en contra de quien cometió el ilícito y no en contra de la entidad bancaria. De ahí que el usuario formulara denuncia, además fue quien propició el ilícito en la medida en que incumplió con la custodia de su usuario y clave, únicos elementos que permitían la transacción.

Hecho de un tercero. El hurto del dinero y los consecuentes perjuicios que aduce el demandante fueron consecuencia de un tercero, quien mediante fraude electrónico que consiste en un mensaje de correo enviado al cliente suplanta al cliente a quien se induce en un mensaje mentiroso que le induce a hacer clic en un vínculo que lo redirección a la página fraudulenta, que simula ser la página legítima del banco. Por lo anterior se rompe el nexo de causalidad y con ello se desvirtúa el trípode de la responsabilidad civil que exonera a la entidad bancaria de responsabilidad.

Cumplimiento contractual y ausencia de elementos de responsabilidad. No puede imputarse culpa a la entidad bancaria, pues no existe falta atribuible ni negligencia, sino que se trata de un hecho de un tercero. El banco cumplió con la verificación de las condiciones de seguridad de la transacción y de los elementos esenciales para la transacción. Tiene contratada la entidad demandada la firma Etek Information Security para la adquisición de los sistemas y elementos

de seguridad necesarios para la protección y prevención de delitos informáticos. El banco invierte grandes cantidades de dinero para cumplir con los requerimientos seguridad informática. El modelo de seguridad de la información que se tiene responde a la norma internacional ISO 17799 y 27001; manejan sistema cifrado de información y sistema que evitan que los datos sean interceptados. La falta de cuidado es imputable al cliente.

Cumplimiento de los protocolos de seguridad por parte de Av Villas. La transacción cumplió con los elementos de seguridad y dado que se llevó a cabo con el usuario y clave personal del cliente no ofreció ningún grado de sospecha que indicara al banco que era objeto de un ilícito. La modificación de las preguntas de seguridad responde a un virus o hacker que el propio cliente activo desde su correo electrónico y que solicitó la notificación de la clave temporal, de ahí que el banco deba ser exonerado de las pretensiones. Sumado al despliegue de seguridad con el que cuenta el banco, al momento de realizar la transacción, se comunica con el cliente quien ante la manifestación de no ser él quien está realizando la transacción, se procede con el bloqueo de la cuenta con lo que se prueba la debida diligencia.

Incumplimiento de condiciones de seguridad por parte del cliente. El cliente incumplió con las recomendaciones para transar seguro por internet tales como no seguir enlaces que se encuentren en correos electrónicos, mensajería instantánea, pop-ups p banners, que podría conducir paginas falsas del banco; ingresar a la página siempre desde la dirección www.bancoavillas.com; evitar realizar operaciones bancarias desde computadores públicos o desconocidos; cuidar las contraseñas de acceso; no responder correos que aparentemente provengan del banco; eliminar correos que provengas de remitentes desconocidos; contar con dos cuentas de correos, una para amigos otra exclusiva para operaciones bancarias. El cliente incumplió el deber de diligencia y cuidado en el manejo de claves y es el responsable del perjuicio, aunado a que no utilizó el servicio de topes personalizados que tiene diseñado el banco para las transacciones; por eso el movimiento financiero fraudulento no ofreció sospecha.

Eximente de responsabilidad pactada. De acuerdo con el contrato de aceptación de servicio que declaró leído y aceptado el cliente tiene indicado en su política 3 que el cliente declara y acepta que es de su exclusiva responsabilidad el acceso a los productos y servicios ofrecidos por el Banco Av Villas y las transacciones que se realizan con su clave secreta ya que sin ello es imposible ingresar al sistema y ordenar cualquier operación. Las operaciones que se realicen con la clave del cliente se entienden realizadas por él por lo que se exonera al banco de tales transacciones. Desde la suscripción del contrato se pactó el eximente de responsabilidad para el banco.

Falta de legitimación por pasiva. Pues se reclama la declaratoria de responsabilidad que no le es imputable al Banco AV Villas, pues la demanda debe dirigirse contra los terceros que cometieron el ilícito penal

Ausencia de causa para pedir. No existe causa de hecho ni de derecho que pueda generar una responsabilidad al banco, quien sólo ha ofrecido un servicio que facilita las transacciones del cliente, los perjuicios sufridos por el demandante obedecen al hecho de un tercero y la omisión de protección y cuidado del propio cliente.

Cualquier otra excepción que resulte probada y que pueda enervar la acción.

La mentada contestación también contiene oposición al juramento estimatorio.

Mediante auto del 06 de abril de 2015 se corrió el respectivo traslado de las excepciones y se estimó improcedente la objeción al juramento estimatorio, dado que no cumple con los parámetros previstos en el artículo 206 del CGP,

Dentro de la oportunidad concedida, el extremo demandante aportó escrito de pronunciamiento frente a las opciones formuladas, y por ser la etapa subsiguiente en el trámite, en auto del 28 de abril de 2015, se corrió el respectivo traslado de las excepciones de mérito, y vencido el mismo se fijó fecha para la audiencia de conciliación prevista en el artículo 101 del CPC, que tuvo lugar el día 24 de agosto de 2015, y en la cual se declaró fracasada la etapa de conciliación, por falta de ánimo conciliatorio de las partes; se agotó el saneamiento del litigio, en el que solo se advirtió que el trámite dado al proceso responde al abreviado del sistema escritural regido por el Código de Procedimiento Civil, como se dejó indicado en la resolución de excepciones previas. A continuación, se procedió a recepcionar los interrogatorios de parte al demandante y al representante legal de la entidad demandada. En la etapa de fijación del litigio, se determinaron los hechos probados y finalmente, se decretaron las pruebas solicitadas por las partes.

Evacuados algunos medios de prueba que habían sido previamente desertados, para continuar con el trámite, el proceso fue asignado al Juzgado Veintinueve Civil Municipal de Oralidad de Medellín quien de cara la transito de legislación en auto del 5 de febrero de 2021, fijó fecha para el día 9 de septiembre de 2021, con el propósito de recepcionar los testimonios faltantes y declarar precluída la etapa probatoria.

Obra grabación de audiencia virtual en el archivo 06 del cuaderno principal, en la fecha prevista, oportunidad en la que se dejó constancia de la inasistencia del extremo demandante y por consiguiente de los testigos decretados a instancia de ese extremo del litigio, por lo que se declaró desistido dicho medio de prueba. Finalmente, se insiste en que el banco debe precisar la respuesta ofrecida al oficio decretado como prueba, para lo cual se concede el término de 30 días y se finaliza la diligencia con la clausura de la etapa probatoria y fijación de fecha para audiencia de alegatos de conclusión y sentencia para el día 29 de noviembre de 2022

2.3. SENTENCIA DE PRIMERA INSTANCIA

En la fecha prevista se llevó a cabo la audiencia, en la que sólo se verificó la comparecencia de la parte demandante; en primera medida, se agotó una etapa de saneamiento, y dado que no se observó apunte al respecto se prosigue con los alegatos de conclusión de cuya oportunidad sólo hace uso el extremo demandado.

Así, escuchado el mentado alegato, se profiere sentencia en la que se declara la responsabilidad civil contractual deprecada en contra del BANCO AV VILLAS y se desestiman la totalidad de las excepciones propuestas. En consecuencia, se condenó a la parte demandada BANCO AV VILLAS al reconocimiento económico en favor del demandante por los siguientes conceptos patrimoniales: la devolución al demandante de todo el dinero que este hubiere cancelado con ocasión al crédito rotativo desembolsado el 15 de marzo de 2013 a través de su cuenta de ahorros 525708181, con inclusión de capital e intereses; pagos que fueron realizados hasta el 13 de mayo de 2014 y suma que deberá ser indexada al día de hoy. Así mismo, la cesación de la ejecución de las obligaciones derivadas de las operaciones financieras producto del crédito rotativo aprobado en favor del demandante el 15 de marzo de 2013 por valor de \$13.450.000. y finalmente, el reintegro a la cuenta de ahorros del demandante Nro. 525708181 de la suma de

\$531.771 debidamente indexados. Sin embargo, las pretensiones correspondientes a la suma de \$800.000 por concepto de daño emergente y el reconocimiento de los perjuicios extrapatrimoniales (perjuicios por la alteración de las condiciones normales de existencia y perjuicios morales) fueron desestimadas. La condena en costas fue impuesta a la parte demandada y a favor de la parte demandante.

Lo anterior fundado en el análisis que pasa a esbozarse.

En primera medida hallándose cumplidos los presupuestos procesales para dictar sentencia de primera instancia, se procedió a hacer un breve recuento de pretensiones y hechos de la demanda; en igual sentido, se formuló el siguiente problema jurídico: Determinar si corresponde o no endilgar responsabilidad civil contractual a la entidad bancaria por el fraude a la cuenta de ahorros y productos financieros de uno de sus clientes, hecha a través del portal de internet, atiende específica y prácticamente al debe profesional de función cuidado y custodia del dinero que se endilga en cabeza de la parte demandada.

El a quo determinó como hechos facticos relevantes los siguientes: que el demandante es titular de una cuenta de ahorros en el Banco Av Villas; que el día 15 de marzo de 2013 iba a realizar una transacción y que una funcionaria le manifestó que su cuenta se encontraba bloqueada, al detectarse por el mismo banco una transacción sospechosa el día anterior, transacción que pretendió efectuarse por la suma de \$1.000.000 y respecto de la cual manifestó el propio demandante que era quien, efecto, iba a realizar dichos movimientos y la empleada del banco le manifestó que el desbloqueo de su cuenta se concretaría el mismo día 15 de marzo de 2013 después del mediodía y que se le daría aviso del desbloqueo. Del interrogatorio de parte rendido por la representante legal del banco está manifestó no tener certeza sobre el bloqueo de la cuenta.

Se destacó también como hecho relevante que el mismo día 15 de marzo de 2013, a las 12:45 de la tarde el demandante manifestó haber recibido una llamada del call center de Av Villas en la que se le pregunta si había realizado una transacción de retiro con tarjeta débito, a lo que contestó que no, que estaba bloqueada su cuenta y que aún no había recibido un aviso respecto del desbloqueo de la misma, que de nuevo le insistieron en la pregunta, para constatar se había realizado una transacción por valor de \$13.450.000, a lo que reiteró la negativa; dada esa circunstancia el funcionario del call center le indicó al demandante que se dirigiera de inmediato a una oficina por temas de seguridad. Al respecto de este hecho, en el interrogatorio de parte practicado al representante legal de la entidad demandada, se le indagó si se había realizado una llamada al demandante que alertaba sobre la transacción, a lo que respondió que, si se habían realizado unas llamadas al titular el día en que se generó dicha transacción, sin poder precisar la hora exacta en que se hicieron las llamadas. Conforme la prueba decretada se requirió a la parte demandada para que aportara al expediente la grabación de las llamadas y no se obtuvo dicha prueba toda vez que la antigüedad de la prueba solicitada no brindó la posibilidad de la aportación de la misma; tampoco la entidad demandada aportó documentos informes o la declaración del empleado que realizó la mentada llamada, para los efectos probatorios correspondientes.

Como tercer hecho relevante consideró el a quo, la manifestación del demandante que recibió una llamada en horas de la tarde del día 13 de marzo de 2013, donde una empleada le informó que la tarjeta ya había sido desbloqueada, esto con posterioridad a la realización de la transacción fraudulenta. El hecho cuarto relevante para lo constituyó que una empleada del Banco le explicó al demandante que el crédito rotativo que tenía a su favor y había sido aprobado

anteriormente, le habían bajado a su cuenta \$13.450.000, suma con la que habían realizado una compra por el aplicativo PSE para el pago de una seguridad social, para una empresa que es ajena al proceso, por valor de \$13.891.771, y por sugerencia de la funcionaria se procedió nuevamente con el bloqueo de su cuenta, pese a que para ese momento ni siquiera sabía que se había levantado el bloqueo anterior, pues no se le había informado. En contraste resaltó que en interrogatorio de parte, la representante legal del banco explicó el hecho de la transacción fraudulenta de la siguiente manera: una persona desde el correo electrónico del demandante a través de su perfil transaccional creó preguntas de seguridad para inscribir una cuenta, el portal transaccional le generó una cuenta por noventa minutos, tiempo en el cual se procedió con la transacción que consiste en retirar del crédito rotativo autorizado al demandante, la suma enunciada, y a continuación se procedió a pagar a través del portal PSE a una cuenta por concepto de prestaciones sociales a una sociedad desconocida en el litigio.

Como otro hecho relevante, se anunció las múltiples reclamaciones hechas por el demandante a la entidad demandada, sin embargo, se le indicó al cliente que las transacciones se realizaron con el usuario y que el banco procedió con la verificación de los datos de seguridad y verificadas las mismas, no es posible acceder a las peticiones del demandante. El último supuesto de hecho relevante lo constituye, es la suspensión de las retenciones como medida cautelar innominada decretada por el juez de instancia y que se efectúa a partir del 13 de mayo de 2014, fecha a partir de la cual no se le han efectuado al demandante retenciones correspondientes a las cuotas del crédito rotativo.

Ahora bien, como presupuestos jurídicos relevantes se enunció jurisprudencia acerca de la responsabilidad civil, sin embargo, para el caso concreto únicamente realiza una pequeña reseña de lo atienen a la responsabilidad civil contractual, particularmente sus presupuestos. Frente a la responsabilidad civil contractual respecto de la actividad financiera, recalca que conforme a la posición jurisprudencial, los clientes o consumidores financiero constituyen la parte débil de la relación contractual y que el banco, en principio, tiene la posición dominante, de ahí la rigurosa imprimación estatal en las prácticas mercantiles, refiere particularmente el tema de la seguridad como un deber de la entidad bancaria y respecto del cliente, recalca que en el ordenamiento positivo las instituciones bancarias ejercen una actividad que es profesional, habitual y de la cual se deriva un provecho económico a la que es inherente una multiplicidad de peligros y riesgos operacionales. Por consiguiente, a la hora de apreciar la conducta de un establecimiento bancario es preciso que se trata de un comerciante experto en intermediación financiera y que maneja recursos ajenos con fines lucrativos en el que se encuentra depositada la confianza colectiva por lo que se le exige obrar de manera cuidadosa, diligente, oportuna dados sus conocimientos especializados en materia bancaria. Por lo que, explicó, en materia de responsabilidad civil de entidades financieras, impera el modelo particular de responsabilidad civil profesional del banco.

Refiere que tratándose de cuentas de ahorro el banco es responsable por el reembolso de las sumas depositadas que hagan personas distintas al titular de la cuenta o de sus mandatarios, sin desconocer que la responsabilidad que se presume respecto de la entidad financiera puede atenuarse, moderarse e incluso excluirse en virtud de la culpa atribuible al titular de la cuenta

Aludió a que el riesgo que se asume con la implementación de servicios financieros mediante plataformas tecnológica, se materializa con el ofrecimiento al cliente del servicio para realizar sus transacciones en línea, sistema que per se, es vulnerable por delincuentes cibernéticos dada la fragilidad inherente a los sistemas electrónicos. De ahí que este conminada la entidad

financiera a adoptar mecanismos de protección de datos de transferencia electrónica con relación a sus usuarios a través de los cuales pueda prevenirse su defraudación; es decir, el banco está sujeto a la responsabilidad que genera para ellos la creación del riesgo del fraude que afecta a sus clientes.

A continuación, refiere la modalidad de fraude que se presentó en el caso concreto a la cual se aludió en la contestación de demanda y en el interrogatorio de parte rendido por la representante legal del banco, denominada “*phishing*”, diseñada para conseguir los datos personales de los usuarios del portal del banco que les permita acceder con las contraseñas de estos a las plataformas correspondientes, para luego indicar que dado que estas acciones fraudulentas constituyen un riesgo inherente a la actividad bancaria cuya ejecución se le exigen altos estándares de calidad, eficiencia, seguridad, fiabilidad y control, tiene que ser atendidos a través de la plataforma correspondiente a cargo del banco o la entidad financiera que pretenda prestar el servicio al usuario de manera voluntaria. Es entonces ineludible su obligación de garantizar la seguridad de las transacciones que autoriza por cualquiera de los medios que el mismo banco le ofrece al usuario, de suerte que los riesgos que se materializan en estos eventos, corren por su cuenta y por lo tanto deben ser asumidas las consecuencias derivadas de ellos, en tal sentido, reparar los perjuicios causados.

Indicó además que independientemente de la obligación de reserva que detenta la parte pasiva o más vulnerable del contrato correspondiente, no es otra que la de tener bajo su custodia y vigilancia las claves que corresponden, más otros riesgos inherentes al desarrollo del contrato de actividad bursátil deben ser asumidas por la entidad financiera, que es quien ocupa la posición dominante en el contrato. Bajo este escenario, subrayó que el banco para exonerarse de responsabilidad debe probar que el hecho fraudulento ocurrió por culpa del cliente o sus dependientes, pues quien alegue la culpa debe probarla, en tanto se presume la buena fe exenta de culpa de la parte pasiva.

Coherente con todo o anterior se ocupó del análisis probatorio, no sin antes precisar que para el *sub lite*, opera el fenómeno de la carga de la prueba, que consiste en que la entidad financiera debe probar la culpa del usuario en la actuación que dio lugar a la ocurrencia del fraude. En ese punto, advirtió la deficiencia probatoria, pues no se halla probada la culpa del demandante de cara a la operación fraudulenta que se concretó con sus productos financieros. Por el contrario, de manera adversa a los intereses de la parte demandada, estimó probado que la entidad financiera al ser titular de la posición dominante y beneficiosa respecto del demandante nada dijo del bloqueo de la tarjeta representativa de la cuenta de ahorros con el cual se efectuaron los pagos a través del portal PSE; tampoco logra justificar por qué habiéndose presentado un bloqueo de la cuenta de ahorros, hecho que no fue desvirtuado en el proceso, no fue impeditivo este supuesto de hecho para la realización de transacciones posteriores, pues pudo haber sido catalogado ese hecho como indicio de movimientos fraudulentos en la cuenta del demandante. En este punto, refirió el interrogatorio de parte absuelto por el representante legal de la entidad bancaria demandada, para referir que en ella ni siquiera dio cuenta de la certeza que tuviera sobre el bloqueo de la tarjeta previo a la transacción sospechosa. Sumado a lo anterior, nada se dijo del momento en que se procedió con el desbloqueo de la cuenta del demandante, ni se procedió con su aviso. Muy a pesar, de que es la propia entidad quien tiene la facilidad probatoria para allegar la evidencia de esos supuestos fácticos.

Cuestiona la falladora de instancia, el hecho de que, pese a encontrarse bloqueada la cuenta del demandante se realizaran actividades fraudulentas y que la entidad financiera no brinde claridad

durante el trámite, en qué momento se produjo el bloqueo y desbloqueo de la cuenta, pese que tiene la posibilidad de hacerlo por ser quien tiene acceso a los datos e información que así permita constatarlo. En el mismo sentido, resaltó la omisión probatoria en relación con las presuntas llamadas que se hicieron al cliente para la autorización de la transacción que se denomina fraudulenta, en la medida en que no aporta la grabación correspondiente, tras la razón de no contar de manera extensiva en el tiempo con el archivo de la grabación, pero tampoco se pronunció a través de la representante legal al respecto, pues al indagarse sobre ese punto adujo sobre la realización de las llamadas al titular, el mismo día en que se generó la transacción, sin contar con el registro correspondiente de las llamadas, ni otro medio probatorio que así pudiera constatar. Máxime que como lo resaltó anteriormente, tampoco obra prueba del descuido que se endilga al demandante en sus transacciones

Resaltó la falladora de primer grado que tanto el hecho del desbloqueo de la tarjeta como la aprobación de la transacción que no corroboró el demandado en la presunta llamada que le hizo el funcionario del banco, fueron asuntos asumidos de manera pasiva por la entidad bancaria, sin proceder a generar un reporte de transacción sospechosa. Así, se halló evidente la falta de diligencia y cuidado de la parte demandada, que le es exigible de manera fehaciente dada la actividad que desempeña y por ser un profesional en esos menesteres, además que deriva un provecho económico que percibe por la ejecución de una actividad que tiene un interés público, de suerte que la responsabilidad por no cumplir con ese deber profesional sólo se resquebraja si por culpa del cuentahabiente o de sus dependientes se produce un pago o se materializa una operación. Y como reiteró, esa circunstancia no se probó en el presente caso.

Concluyó entonces que existe en el proceso orfandad probatoria de los mecanismos de seguridad adoptados para evitar la ocurrencia del riesgo derivado de la transferencia electrónica, así como de la falta y diligencia del cliente en el manejo de su clave. Aun cuando se diera como probado que las plataformas de Av Villas cuentan con la seguridad debida para la realización de operaciones mediante el portal transaccional electrónico, la sola ocurrencia del suceso no imputable a la falta de cuidado del demandante, resulta un deber inexcusable de la entidad financiera precaver el suceso y evitarlo. Lo anterior, con el agravante que lo ocurrido no es un caso aislado, sino que es un hecho plenamente conocido por la entidad financiera, habida cuenta que ya se tenía conocimiento de la forma como se presenta dicha modalidad de fraude y que obedece a un patrón detectado por la entidad financiera.

Por lo dicho se desestimaron todas las excepciones propuestas por la entidad demandada, en la medida en que no le era endilgada a la parte demandante funciones probatorias que para el presente asunto son exclusivas de la demandada, a quien además le correspondía, no sólo probar que cuenta con condiciones de seguridad, sino que para el presente caso hubieren operado de esa manera y que atiendan al riesgo que se crea con la actividad que se oferta a los clientes de transacción electrónica.

Por lo dicho, halló la autoridad judicial de primera instancia probados los presupuestos para declarar la responsabilidad contractual de la entidad demandada, pues es claro que existe un vínculo entre quien como demandante reclama la debida conducta de la parte demandada, esto es la existencia del contrato y ello se probó con la celebración del contrato de servicios electrónicos de los productos financieros de propiedad del demandado. Así mismo, se evidenció la inexecución o ejecución retardada de alguna de las obligaciones contractuales como lo es en el presente caso, la obligación de seguridad que le es atribuible a la entidad financiera. Finalmente, el daño, producto de la ocurrencia de la transacción fraudulenta también fue

probada.

Hallada entonteces probada la responsabilidad contractual en cabeza de la entidad financiera, se ocupó el a quo de verificar la procedencia de cada una de las pretensiones consecuenciales derivadas de ella, que fueron reclamadas por el demandante, para establecer su reconocimiento, que sólo opera por aquel detrimento que haya sufrido como una consecuencia directa de la ocurrencia de la transacción fraudulenta. Bajo esa tesis negó los gastos de representación reclamados a título de daño emergente por valor de \$800.000. Ahora, frente a la suma de dinero que constituyó el importe de la operación fraudulenta, equivalente a \$13.891.771, se ordenó la devolución por parte del Banco y a favor del demandante de todo el dinero que hubiere cancelado con ocasión al crédito rotativo desembolsado a través de su cuenta de ahorros con inclusión del capital e intereses, pagos que en virtud de la medida cautelar decretada en el proceso, se realizaron por el demandante hasta el 13 de mayo de 2014; en igual sentido, se condenó a la devolución de las sumas que hubiere consignado el demandante o que se le haya deducido de sus cuentas correspondientes, indexada al día en se profirió la sentencia. Consecuente con la decisión, se declaró también la cesación de la ejecución de las obligaciones derivadas de las operaciones financieras producto del crédito rotativo aprobado en favor del demandante. Dado que la operación fraudulenta lo fue por un monto total de \$13.891.771, y el valor del desembolso equivale a \$13.450.00, y en atención a que debió retirarse de su cuenta la suma de \$531.771, ese monto fue el que se dispuso reintegrar al demandante debidamente indexados.

Frente a los perjuicios reclamados por la alteración a las condiciones de existencia, advirtió el juez de primer grado, que no había prueba de su ocurrencia y no es de los que se presuman para el caso concreto. En igual medida, no se existió actividad probatoria en relación con los perjuicios extrapatrimoniales reclamados, de suyo que negó la pretensión en relación con esos conceptos.

Ante esta decisión, la parte demandada formuló recurso de apelación, y en esa oportunidad indicó como reparos concretos los siguientes:

La valoración de la prueba, en relación con la culpa del demandante, pues en el interrogatorio de parte que absolvió éste, confesó que la información utilizada dentro de la transacción fraudulenta es su información personal.

Adicionalmente no se valoró la prueba aportada por la entidad demandada al momento del interrogatorio de parte absuelto por el representante legal Banco, contenida en un CD, donde obran los siguientes documento: archivo que contiene el historial transaccional del cliente entre el 15 de marzo de 2012 y 15 de marzo de 2013 donde evidencia su perfil de comerciante; también un archivo en que se observan las claves temporales que fueron remitida al celular y correo electrónico registrado por el cliente, que desmiente la afirmación de no realizar transacciones electrónicos porque las claves personales las solicita por otro medio diferente al utilizado para el fraude. Obra allí también, la bitacora transaccional del cliente, los extractos de la cuenta y el pantallazo de la transacción objeto de debate donde se puede observar que la misma fue ejecutada con la clave y usuario del cliente; sobre esta última prueba, resalto que tal como se dejó dicho en interrogatorio por el representante del banco, no se avizó riesgo en las transacciones realizadas por el cliente.

Anotó que el bloqueo anterior que se generó al producto del cliente - demandante fue por una

transacción en cajero electrónico y no por transacción electrónica, por lo que la alarma la generaron circunstancias diferentes.

Alega que si se probaron las medidas de seguridad adoptadas por el banco y que obran en el plenario las dos investigaciones internas que se realizaron, de las que se desprende que en el suceso fraudulento no hubo vulneración al sistema o plataforma de banco.

Se duele también la inconforme, que la Juez de primer grado, no hubiere valorado de la conducta del cliente quien como comerciante traía un historial transaccional continuo que fue aportado como prueba y que permite concluir que es una persona de múltiple actividad financiera que no tenía limite en las transacciones y que el desembolso realizado desde le crédito rotativo estaba dentro de los límites, entonces, al no observarse de riesgo o prevención frente a la transacción, por eso se concretó la operación cuestionada.

Finalmente repudia la valoración probatoria que se hizo a la declaración rendida por la representante legal del banco pues si bien en la misma se aludió a una modalidad de fraude, no dijo que hubiere sido la misma que se presentó en el actual caso, pues no hay evidencia que el demandante hubiere recibido un correo electrónico que proviniera de una plataforma fraudulenta, y no existe conclusión técnica producto de alguna investigación electrónica, que permita concluir que el demandante fue víctima de este tipo de fraude y que se hubiere vulnerado su información

2.4 APELACIÓN DE SENTENCIA

La apoderada de la parte demandada, mediante correo electrónico del 2 de diciembre de 2022, remitió escrito de sustentación del recurso de apelación en el cual expuso:

Que contrario a lo estipulado en primera instancia, la entidad bancaria demandada, cumplió a cabalidad con la debida diligencia, en cuanto al deber de un manejo seguro de la información y protocolos de seguridad. Para sustentar esa afirmación, asegura que de las pruebas practicadas en el proceso, se desprende que el BANCO AV VILLAS cuenta con un sistema de prevención de fuga de la información llamado “Websense Content Portection suite” y en soluciones de transferencias de archivos con el programa “Secure Transport Tumbleweed” y actualización de software suscription”; que dichos programas cuentan con la más alta tecnología del mercado que no solo brindan seguridad en operaciones y transacciones, si no que cuentan con la mejor calidad del mercado, proporcionándoles seguridad a los clientes para el manejo de transacciones y operaciones. Sumado a lo dicho, el Banco Av Villas cuenta con medidas de seguridad en el portal de internet basados en los estándares internacionales ISO 17799 y 27001; y una política estricta de seguridad que ha sido aprobada por un comité de riesgos.

De acuerdo con lo anterior, insiste en que en el trámite si se logró demostrar que las actividades comerciales que realiza el banco, poseen los más altos estándares de seguridad en el mercado, sowlfare y programas que se encargan de permitir el flujo seguro y vigilado de la información, y que dichos sistemas no fueron vulnerados ni puestos en peligro al momento de la ocurrencia de los hechos descritos en la demanda. Señaló al momento de generar claves temporales, el sistema con que cuenta su representada, ofrece seguridad al cliente quien para la transacción debe efectuar conformación desde su correo electrónico personal y registrado ante el Banco, situación que en le caso bajo examen se dio con total normalidad.

Insiste en que la ocurrencia del hecho que genera el daño es culpa exclusiva del demandante por actos imputables directamente a este y a sus dependientes, pues el cliente tiene la obligación de mantener una estricta seguridad y privacidad de su usuario y sus claves de acceso, ya que para el momento de la inscripción al servicio de Banca Personal Por Internet fue necesaria la digitación de datos como número de identificación, número de producto a inscribir, clave secreta de la tarjeta y número de la tarjeta, dato que fueron verificado en las investigaciones internas que hizo el Banco a fin de analizar cómo se habían realizado los movimientos bancarios del demandante el día 15 de marzo de 2013, que arrojó que la operación fue efectuados de manera normal y con los datos usuales personales del cliente, que son de su único conocimiento y custodia. Sumado a esa circunstancia, indica que cuando el cliente decidió suscribir un contrato para la realización de operaciones por internet, asumió de las políticas que rigen al interior de la compañía, dentro de las cuales se encuentra estipulado que el cliente se obliga a mantener la información sensible y personal, bajo estricta seguridad y confidencialidad, por lo que no puede compartirla y ni darla a conocer a terceros. Por consiguiente, la ocurrencia del hecho, es producto de la negligencia e indebido cuidado de la información por parte del demandante quien, compartió indiscriminadamente su información personal y claves e incumplió con dicha conducta las obligaciones adquiridas a la firma del contrato.

Como mencionó al iniciar su reproche, cuenta la entidad demandada con programas y sistemas que permiten advertir riesgos transaccionales, sin embargo, pese a contar con esos mecanismos, no se identificó en el caso de marras un posible riesgo o violación a la seguridad, en tanto la transacción fue realizada con el usuario y contraseñas del demandante, más aún cuando se enviaron claves electrónicas de acceso al correo personal del cliente, y se absolvieron las preguntas de seguridad cuya respuestas son de uso exclusivo del cliente.

Reclama que sea tenido en cuenta el material probatorio aportado, mediante el cual se evidencia el historial de transacción del cliente, extractos de la cuenta del cliente, pantallazo de la transacción objeto de discusión, donde consta que esta fue ejecutada con la clave y usuario del cliente, correo electrónico denominado “RE: Claves OTP JUAN FELIPE YASSER ESCOBAR” el cual contiene las claves OTP remitidas a los canales autorizados por el cliente, que son, el celular y el correo electrónico. Todo ello para que se constate que la transacción fue realizada con la habitualidad que el cliente acostumbra hacer, y por consiguiente el banco no encontró alerta que pudiera significar un posible fraude o delito.

Afirma que el Banco Av Villas ha cumplido a cabalidad con la debida diligencia que le corresponde, pues ha mantenido bajo vigilancia continua las transacciones y movimientos en las cuentas de los clientes y los alerta cuando se presenten posibles operaciones que se puedan tornar sospechosas, empero, insiste en que en el caso concreto, no se logró identificar una operación que pudiera representar una señal de alerta pues la transacción fue realizada con la habitualidad que el cliente acostumbra y sus datos personales, de ahí que no sea dable afirmar que la entidad bancaria omitió pronunciarse sobre un posible riesgo operacional, pues en ese evento no se configuró una alerta en tanto el procedimiento no presentaba vicios, errores u operaciones sospechosas que nos pudieran permitir deducir que el cliente era víctima de un hacker o virus.

Refiere que el bloqueo de la cuenta del demandante no fue tomado como alerta o indicio de hechos fraudulentos porque el cliente se había comunicado previamente con el banco para autorizar el desbloqueo de su clave. Por esa razón, y pese a no tener las grabaciones telefónicas de la conversación, porque las mismas por ley deben eliminarse cada determinado tiempo, el Banco tiene plena conciencia de la importancia de la seguridad y los peligros que la era

tecnológica puede traer, por estos motivos, itera que el cliente fue contactado para informarle del bloqueo de su cuenta, quien posteriormente y a su juicio solicitó el desbloqueo de la misma para ser utilizada.

Ahora, frente a la afirmación efectuada en la decisión de reprocha, relativa a que la entidad bancaria desconoció un posible caso de 'fraude por phishing', indicó que en el proceso el demandante en ningún momento hizo alusión a ser víctima de este tipo de delitos y tampoco hay prueba de su ocurrencia en el caso concreto, y aun cuando resulte palmario que el demandante fue víctima de un hurto de dinero realizado mediante medios electrónicos que nada tienen que ver con el ente financiero, ese hecho no fue materializado por negligencia que le sea imputable, pues como ha sostenido, su actuar atendió la debida diligencia en todo momento, por lo que resulta errado endilgarle responsabilidad civil.

Finalmente, admite que aun cuando en principio la responsabilidad recae sobre las entidades bancarias por considerarse como la parte más fuerte de la relación, conforme la jurisprudencia patria, la carga de la responsabilidad no le es absoluta, y en esa medida constituye un deber del juez analizar todas las situaciones y el contexto tanto del demandado, así como las acciones y conducta del demandante que pudieran determinar una eventual negligencia de cuidado de la información por parte de este último. Que el banco probó los estándares y mecanismos de seguridad con que cuenta y que la mera ocurrencia del hecho fraudulento en la transacción cuestionada, no se traduce en negligente en el desempeño de las actividades financieras. Contrario a lo que estableció la Juez de primer grado, la negligencia es atribuible al demandante por el uso indebido de su información personal, pues, tal como se concluyó en las investigaciones realizadas con ocasión de la reclamación del cliente, éste incumplió su obligación de no divulgar o exponer el usuario y la clave.

Coherente con las razones expuestas, solicitó que se valorara la prueba de manera completa y no parcializada, y que sean tenidos en cuenta los archivos aportados con el historial transaccional del cliente, extractos de la cuenta del cliente, pantallazo de la transacción objeto de discusión, donde consta que esta fue ejecutada con la clave y usuario del cliente, correo electrónico denominado RE: Claves OTP JUAN FELIPE YASSER ESCOBAR el cual contiene las claves OTP remitidas a los canales autorizados por el cliente, a saber el celular y el correo electrónico. Esto con la finalidad de probar que el banco cumplió con todas las condiciones de seguridad y que no habían señales de posibles fraudes electrónicos, por lo que la transacción fue realizada con las claves de acceso que solo el cliente debía conocer, cuyo descuido constituye la única causa del fraude.

Con fundamento en los anteriores motivos pidió revocar la sentencia de primera instancia, y en su lugar negar las pretensiones de la demanda.

2.5 TRÁMITE SEGUNDA INSTANCIA

En vista de que la sustentación del recurso se presentó en tiempo por la parte demandada, el A quo, concedió el recurso de apelación de la sentencia en el efecto devolutivo en la audiencia en que se emite la decisión cuestionada, en razón a lo cual fue repartido el expediente a este Despacho para su respectivo trámite, y ajustado a la previsión normativa contenida en la ley 2213 de 2020 en su artículo 12, se procedió con su admisión por auto del 13 de febrero de 2023; el día 23 de febrero se corrió traslado por cinco días al apelante, quien en su oportunidad presentó escrito de sustentación.

En el mentado escrito, la apoderada judicial del Banco Av Villas reiteró los argumentos en que sustentó la apelación ante el Juez de primera instancia y por consiguiente reiteró su solicitud de revocar la decisión adoptada por esa autoridad judicial.

Posteriormente, en la fecha 07 de marzo de 2023, se corrió traslado del escrito de sustentación a la parte no apelante, y al respecto no se hizo pronunciamiento alguno, razón por la cual corresponde proferir la presente sentencia escrita.

3. CONSIDERACIONES

3.1. PRESUPUESTOS PROCESALES: Sea lo primero recalcar, que los presupuestos procesales necesarios para proveer una decisión de fondo se reúnen. A la jurisdicción ordinaria le corresponde conocer del asunto que nos ocupa; la competencia en primera instancia se radicó en el Juzgado Dieciocho Civil Municipal de Oralidad de Medellín y posteriormente, en virtud de las medidas de descongestión se trasladó su conocimiento al Juzgado Veintinueve Civil Municipal de Oralidad de esta misma ciudad, en virtud de la cuantía, que corresponde a la de menor, en razón al monto de las pretensiones, al domicilio de las partes y al lugar de ocurrencia de los hechos. De otro lado, los extremos litigiosos gozan de capacidad para ser parte. Finalmente, la capacidad para comparecer en litigio se reúne, por cuanto no existe prueba que pueda demostrar lo contrario ya que tanto la parte demandante, como la demandada estuvieron representadas por profesionales del derecho idóneos para el caso en particular.

Como el apelante único se encuentra protegido por la garantía Constitucional de la *no reformatio in pejus* y señala al Juez de segunda instancia los precisos límites de la decisión que en caso haya de tomarse, el fallo de segunda instancia únicamente se ocupará de los puntos de disenso que indica el recurrente. Coherente con ello, y al tenor de lo dispuesto en el inciso final del artículo 327 del C.G.P., que dispone que el apelante deberá sujetar su alegación a desarrollar los argumentos expuestos ante el juez de primera instancia, esta segunda instancia restringirá su decisión al análisis de los reparos formulados al momento de la interposición de la alzada y su sustentación presentados en este trámite.

La inconformidad del recurrente radica en la indebida valoración probatoria realizada por la Juez de primera instancia, que condujo a erradas conclusiones para sustentar la declaratoria de responsabilidad civil contractual en cabeza de Av Villas, con cuya determinación, desconoció que obra evidencia fehaciente en el plenario de que la entidad financiera demandada probó la diligencia y cuidada en la ejecución del contrato celebrado con el demandante, al allegar la prueba de que cuenta con sistemas, mecanismos y protocolos de seguridad que garantizan el manejo seguro de la información y las transacciones. Así mismo, no se valoró que la ocurrencia del fraude en la transacción cuestionada es producto de la culpa exclusiva de la víctima, a quien se le atribuye negligencia e indebido cuidado de la información personal y las claves, con cuya conducta incumplió las obligaciones adquiridas a la firma del contrato. Contrario a lo sostenido en la primera sede de análisis, el banco cumplió a cabalidad con sus deberes contractuales y legales de vigilancia respecto de las transacciones realizadas por el demandante.

3.2. EL PROBLEMA JURÍDICO: Establecido el marco dentro del cual se desarrolló la controversia, así como el sentido de la sentencia impugnada y las razones de inconformidad de la parte recurrente, este Despacho deberá determinar si confirma o revoca la sentencia de primera instancia que acogió parcialmente las pretensiones de la demanda al declarar la

responsabilidad civil contractual del Banco Av Villas por la operación fraudulenta de la fue víctima el demandante el día 15 de marzo de 2013, por valor total de \$13.891.771. Para tal efecto y dado que lo se cuestiona es la indebida valoración probatoria realizada en primera instancia, se ocupará este Despacho de verificar si en con la evidencia que obra en el plenario asiste razón a la entidad apelante, pues de dichos medios de conocimiento puede evidenciarse que la entidad bancario demandada, cumplió a cabalidad sus deberes contractuales y legales de seguridad y por consiguiente la culpa exclusiva víctima a cuya causa se atribuye la operación fraudulenta, quedó al descubierto con el caudal probatorio recaudado en el litigio.

En aras de resolver el problema jurídico formulado, se analiza el siguiente

3.3. FUNDAMENTO LEGAL Y JURISPRUDENCIAL:

Es indiscutible la trascendencia de la actividad financiera en la economía, de ahí que el artículo 335 de la Constitución Política consagra que a la par de la bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e inversión de los recursos de captación *“son de interés público y sólo pueden ser ejercidas previa autorización del Estado, conforme a la ley, la cual regulará la forma de intervención del Gobierno en estas materias y promoverá la democratización del crédito”*. Precisamente, el Decreto 663 de 1993, con el que se compilaron todas las normas que conforman el Estatuto Orgánico del Sistema Financiero, señalan como integrantes de éste a los establecimientos de crédito, de los cuales hacen parte los establecimientos bancarios, que en el artículo 2º se definen como las *“instituciones financieras que tienen por función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término, con el objeto primordial de realizar operaciones activas de crédito”*.

La importancia de tal actividad en el orden social y económico, justifica el establecimiento de controles y políticas restrictivas en su desarrollo, amén de llevar ínsita la exigencia para las instituciones financieras de un mayor grado de diligencia y profesionalismo, porque la actividad que desarrollan además de profesional, tiene los rasgos de ser habitual, masiva y lucrativa, requiere de una organización para ejecutarla y del conocimiento experto y singular sobre las operaciones que comprende, así como de los productos y servicios que ofrece al público, razón por la cual los estándares de calidad, seguridad y eficiencia que se le reclaman, son más altos que los exigidos a un comerciante cualquiera.

Toda vez que los adquirentes de los productos ofrecidos por los bancos, entre los cuales están los titulares de cuentas corrientes y de ahorro, constituyen la parte débil de la relación y el Banco, en principio, tiene una posición dominante, la intromisión estatal en esa dinámica mercantil tiene entre sus objetivos que *“esté en concordancia con el interés público”*; se tutelen preferentemente las expectativas de ahorradores y depositantes; y las operaciones *“se realicen en adecuadas condiciones de seguridad y transparencia”*, al tenor del artículo 46 ibídem.

En ese sentido, la Corte Suprema de Justicia ha sostenido que: (...) debe tenerse en cuenta que ‘a la luz del artículo 335 de la Constitución Política la actividad financiera es «de interés público» y que, de acuerdo con precedentes jurisprudenciales, ha sido catalogada como un servicio esencial (...) “Tampoco ha de negarse que las empresas dedicadas a esa labor en principio ostentan una posición dominante, pues según se sabe, «la banca en sus diferentes manifestaciones es una compleja amalgama de servicio y crédito donde las empresas financieras que la practican disponen de un enorme poderío económico que ‘barrenando los principios

liberales de la contratación' como lo dijera un renombrado tratadista (...), les permite a todas las de su especie gozar de una posición dominante en virtud de la cual pueden predeterminar unilateralmente e imponer a los usuarios, las condiciones de las operaciones activas, pasivas y neutras que están autorizadas para realizar... (CSJ SC, 30 Jun. 2001, Rad. 1999-00019-01).

Adicional a lo anterior, dentro de los principios reconocidos por el estatuto mercantil se encuentra el de la buena fe que además fue instituido como imperativo de conducta en las distintas operaciones comerciales. En ese sentido, el artículo 871 estatuyó que *“los contratos deberán celebrarse y ejecutarse de buena fe y, en consecuencia, obligarán no sólo a lo pactado expresamente en ellos, sino a todo lo que corresponda a la naturaleza de los mismos, según la ley, la costumbre o la equidad natural”*. En el libro cuarto del Código de Comercio se regulan los “contratos y obligaciones mercantiles”, dedicando el título XVII a los “contratos bancarios”, entre los cuales están el de cuenta corriente (arts. 1382 a 1392) y el de depósito de ahorro (arts. 1396 a 1398). Antiguamente esas dos clases de convenios contaban con diferencias puntuales en su manejo, como el que en las cuentas corrientes se impartieran órdenes de pago mediante cheques, por lo general en favor de terceros; se autorizaran cupos de sobregiro con cargo de pagar intereses, y se enviara una información detallada de los movimientos en extractos periódicos. Por su parte, en las de ahorro, se manejaban libretas en poder del ahorrador, donde se dejaban notas de los depósitos y retiros que él mismo o la persona expresamente autorizada hicieran, además del pago de intereses sobre saldos. No obstante, esa situación cambió con el transcurso del tiempo, como consecuencia de las exigencias del mercado financiero, unificándose en cierta medida la forma de operar ambas como acontece con la entrega de tarjetas débito para pagar en establecimientos de comercio y tener disponibilidad inmediata de moneda, indistintamente de que se trate de una u otra; los movimientos entre diferentes cuentas de un mismo titular, en la misma o diferente entidad; las transferencias a distintos cuentahabientes y el reporte instantáneo de la información.

En ambos contratos, la institución bancaria no solo tiene la obligación de custodia de los dineros recibidos del depositante, sino de garantizar la seguridad de los servicios que ofrece y de las operaciones que permite realizar en relación con tales depósitos, labores en las que, como las demás inherentes a su actividad, debe obrar con la diligencia propia de un profesional, de tal forma que el sector no pierda la confianza del público. En ese sentido, se ha indicado que la seguridad es uno de los deberes significativos en la relación banco – cliente. *“La obligación de seguridad puede considerarse como aquella en virtud de la cual una de las partes del contrato se compromete a devolver al otro contratante, ya sea en su persona o en sus bienes, sanos y salvos a la expiración del contrato, pudiendo ser asumida tal obligación en forma expresa por las partes, ser impuesta por la ley, o bien surgir tácitamente del contenido del contrato a través de su integración sobre la base del principio de buena fe”* (BARBIER, Eduardo Antonio. Contratación Bancaria, Tomo I, Consumidores y usuarios, Buenos Aires: Editorial Astrea, 2º Edición, 2002, pág. 42.). De ahí que a la institución de depósito se le haya exigido responder por las irregularidades en el manejo de los dineros dejados a su cuidado, por el pago de cheques falsificados o alterados en su cantidad (art. 1391 C.Co.) si se trataba de cuentas corrientes, o por “el reembolso de sumas depositadas que haga a persona distinta del titular de la cuenta o de su mandatario” si se refería a las de ahorro (art. 1398 C.Co.).

Por otra parte, entre el Banco y sus clientes se entabla una relación de consumo, en la cual los últimos son reconocidos como la parte débil, de ahí que el ordenamiento jurídico promueva su protección y exija a la entidad un proceder consonante con el interés colectivo trascendente de protección al consumidor que emana de lo estatuido por los artículos 78 y 335 de la Constitución

Política, lo que justifica la serie de obligaciones, cargas y conductas exigibles a dicho profesional, amén de un régimen de responsabilidad diferente del común.

En razón de lo anterior y a efectos de resolver el ataque propuesto contra la sentencia impugnada, es necesario que se aborde la temática de la responsabilidad de los bancos por las irregularidades en el manejo de los dineros dejados a su cuidado, en razón al desarrollo jurisprudencial y doctrinal que aquella ha tenido.

Las nuevas tecnologías y el riesgo de la actividad bancaria:

Entre los avances tecnológicos que han sido incorporados a la actividad de la banca en los últimos años para permitir que las operaciones bancarias se efectúen con mayor agilidad, se destacan los referentes a la modernización de la distribución de productos y servicios financieros, lo que determinó el paso de las oficinas físicas de las sucursales a la atención al cliente por otros canales transaccionales como los cajeros automáticos, los receptores de cheques, los receptores de dinero en efectivo, los sistemas de audio respuesta, los centros de atención telefónica, los sistemas de acceso remoto para clientes (RAS), el internet y, las aplicaciones en dispositivos móviles. Todos esos medios de interacción entre los usuarios del sistema financiero y las entidades que lo integran, algunos implementados con anterioridad a los hechos que motivaron el proceso, requieren para su correcto funcionamiento y el cumplimiento de los fines que legal y contractualmente tienen asignados, rigurosos esquemas de seguridad y protección de la información que por ellos circula, pues a través suyo se realiza la disposición de los recursos monetarios de los ahorradores.

Sucede que a la par que las tecnologías de la información han ampliado enormemente las posibilidades de comunicación y dinamizan las relaciones comerciales, el tratamiento automatizado de datos incrementa los riesgos de ocurrencia de hechos ilícitos que ocasionan daño a los haberes patrimoniales de los clientes de las entidades financieras. En ese sentido, se ha dicho que la difusión de la informática en todos los ámbitos de la vida social ha determinado que se le utilice como instrumento para la comisión de actividades que lesionan intereses jurídicos y entrañan el consiguiente peligro social.

La circunstancia de que internet sea una red abierta y pública, hace que esté caracterizada por una inherente inseguridad, pues eventualmente cualquier transferencia de datos puede ser monitoreada por terceros, lo que incrementa la potencialidad de pérdidas y defraudaciones, cuyos patrones de operación, por lo menos en lo que atañe a la banca electrónica, cambian constantemente y se manifiestan a través de la alteración de registros encaminada a la apropiación de fondos; la suplantación de la identidad de los usuarios, y la simulación de operaciones, compras y préstamos. Sin embargo, no es posible ignorar que se trata de riesgos que son propios de la actividad asumida por las entidades y corporaciones que participan en el comercio, entre ellas los Bancos, de la cual obtienen grandes beneficios económicos, pues son estos los que para disminuir costos y obtener mejores rendimientos, han puesto al servicio de sus clientes los recursos informáticos y los sistemas de comunicaciones a través de la red, en una estrategia de ampliación de la oferta y cobertura de productos y servicios financieros.

Es natural y obvio que la implementación de medios como el portal virtual de transacciones, si bien requiere de una inversión para su operación y mantenimiento, genera un lucro para la entidad, en la medida en que atrae un mayor número de clientes y de operaciones bancarias. No obstante, el uso de este lleva ínsito el riesgo de fraude electrónico, el cual es de la institución

financiera precisamente por la función cumplida por las instituciones financieras y el interés general que existe en su ejercicio y la confianza depositada en él, lo que determina una serie de mayores exigencias, cargas y deberes que dichas entidades deben cumplir con todo el rigor; por el provecho que obtiene de las operaciones que realiza; por ser la dueña de la actividad, la que - se reitera- tiene las características de ser profesional, habitual y lucrativa; y además, por ser quien la controla, o al menos, a quien le son los exigibles los deberes de control, seguridad y diligencia en sus actividades, entre ellas la de custodiar dineros provenientes del ahorro privado.

El riesgo, entonces, se materializa con el ofrecimiento a los clientes de una plataforma tecnológica para realizar sus transacciones en línea, la cual puede ser vulnerada por delincuentes cibernéticos a través de diversas acciones, atendida la vulnerabilidad inherente a los sistemas electrónicos. Por eso, por una parte las instituciones financieras están compelidas a adoptar mecanismos de protección de los datos transferidos en relación con sus usuarios, a través de los cuales pueda prevenirse la defraudación, pues para el momento en que estos son detectados, generalmente, ya se ha causado el daño patrimonial, y por otra, están sujetas a la responsabilidad que acarrea para ellas la creación de un riesgo de fraude que afecta a sus clientes, a disposición de los cuales ha dispuesto su plataforma y recursos tecnológicos.

El tema de seguridad de la información y su adecuada gestión por las organizaciones privadas ha sido una constante preocupación para estas y para el sistema jurídico. Para la época en que sucedieron los hechos se hallaba vigente la Circular 052 de 2007 dictada por la Superintendencia Financiera sobre *“Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios”*, y también existía una norma técnica colombiana (NTC), la cual de conformidad con el Decreto 2269 de 1993 es un *“documento establecido por consenso y aprobado por un organismo reconocido, que suministra, para uso común y repetido, reglas, directrices y características para las actividades o sus resultados, encaminados al logro del grado óptimo de orden en un contexto dado. Las normas técnicas se deben basar en los resultados consolidados de la ciencia, la tecnología y la experiencia y sus objetivos deben ser los beneficios óptimos para la comunidad”*.

La Norma Técnica Colombiana es aplicable a todo tipo de organizaciones públicas y privadas, como, por ejemplo, empresas comerciales, agencias gubernamentales y entidades sin ánimo de lucro. Desde luego, entre ellas se encuentran las instituciones financieras y aunque no es obligatoria ni constituye medio de prueba, fija un estándar o referente en cuanto a lo que se espera de un sistema de gestión de seguridad de la información y la implementación de controles que permitan preservar la confidencialidad de datos, entre otros aspectos.

En cuanto al riesgo derivado del manejo de información, establece que a cada institución le corresponde, entre otras cosas: *“definir el enfoque organizacional para la valoración del riesgo; (...) Identificar los riesgos”*, labor en la que es preciso *“1) identificar los activos dentro del alcance del SGSI y los propietarios de estos activos. 2) identificar las amenazas a estos activos. 3) identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas. 4) Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos”* para después analizar y evaluar los riesgos lo que comprende: *“1) valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos. 2) valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados*

con estos activos, y los controles implementados actualmente. 3) estimar los niveles de los riesgos. 4) determinar la aceptación del riesgo o la necesidad de su tratamiento” y por último “f) Identificar y evaluar las opciones para el tratamiento de los riesgos”.

También indica la Norma Técnica Colombiana que, entre las acciones a realizar para tratar los riesgos en el ámbito de seguridad de la información, se encuentran las de “1) *aplicar los controles apropiados. 2) aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos (véase el numeral 4.2.1, literal c); 3) evitar riesgos, y 4) transferir a otras partes los riesgos asociados con el negocio, por ejemplo: aseguradoras, proveedores, etc”.*

Tales contingencias o eventualidades son consideradas como puramente operacionales y en una clasificación muy básica se les relaciona con las amenazas a los sistemas de información que aparejan “*pérdida de integridad de los datos, pérdida de la privacidad de los datos, pérdida de servicio y pérdida de control”*, e imponen, de modo obligatorio e ineludible, la adopción de medidas que permitan alcanzar un grado de seguridad y confianza en la circulación electrónica de la información y particularmente en las transacciones realizadas por ese canal. El concepto de “seguridad de la información” comprende los de “*preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad”*.”

Por otra parte, entre los objetivos de control y controles que una organización debe contemplar en su sistema de gestión del riesgo, se destacan precisamente los relacionados con las transacciones electrónicas y comerciales, son estos los de 1) garantizar la seguridad de los servicios de comercio electrónico, y su utilización segura; 2) Que la información involucrada en el comercio electrónico que se transmite por las redes públicas debe estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada, y 3) La información de las transacciones en línea “*debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje”*.”

En cuanto al control de acceso, las organizaciones tienen el deber de: 1) Brindar protección a los «puertos de configuración y diagnóstico remoto», el «acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado»; 2) «separar los grupos de servicios de información, usuarios y sistemas de información en las redes»; 3) «restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio» tratándose de redes compartidas; 4) «implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio; y en lo que atañe al acceso al sistema operativo, las entidades están compelidas a «evitar el acceso no autorizado a los sistemas operativos», «el acceso... se debe controlar mediante un procedimiento de registro de inicio seguro», «Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario», «Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas» y se deben prever la suspensión de sesiones con un determinado período de inactividad, y la limitación del tiempo de conexión a la red.

En suma, los Bancos al ofrecer a sus clientes la prestación de servicios bancarios a través de un

portal de internet, las medidas de precaución y diligencia que le son exigibles no corresponden a las mínimas requeridas en cualquier actividad comercial, sino a aquellas de alto nivel que puedan garantizar la realización de las transacciones electrónicas de forma segura, por lo que se impone la implementación de herramientas, instrumentos o mecanismos tecnológicos adecuados, idóneos y suficientes para evitar la contingencia de la defraudación por medios virtuales o minimizar al máximo su ocurrencia, que impone blindar de la debida seguridad el entorno web en que se desarrolla, los elementos empleados, las contraseñas y claves, el acceso al sistema, la autenticación de los usuarios, la trazabilidad de las transacciones, el sistema de alertas por movimientos sospechosos o ajenos al perfil transaccional del cliente y el bloqueo de cuentas destinatarias en transferencias irregulares, de ser el caso.

Entre las modalidades de fraude electrónico más conocidas se encuentran las de interceptación de datos del medio de pago electrónico y de su titular en los canales virtuales por los cuales circula esta información, y la obtención de esta al extraerla de las bandas magnéticas de las tarjetas débito o de crédito, o del chip de la tarjeta inteligente, deben incorporar mecanismos detectores en cajeros electrónicos y datáfonos. Tales situaciones, en principio, no suponen un descuido o negligencia del cliente o titular del medio de pago, pues el fraude electrónico puede ocurrir con independencia del cuidado en la custodia de las tarjetas y aún de las claves, como a continuación se explica al mencionar las formas de defraudación más empleadas en ambientes enteramente virtuales.

La responsabilidad en este tipo de fraudes:

De la exposición que precede, queda claro que en el caso de defraudación por transacciones electrónicas, dado que tal contingencia o riesgo es inherente a la actividad bancaria la cual es profesional, habitual y lucrativa, cuya realización requiere de altos estándares de diligencia, seguridad, control, confiabilidad y profesionalismo, que también tienen que ser atendidos en materia de seguridad de la información que sea transmitida por esa vía, lo que hace innegable e ineludible su obligación de garantizar la seguridad de las transacciones que autoriza por cualquiera de los medios ofrecidos al público y con independencia de si los dineros sustraídos provienen de cuentas de ahorro o de cuentas corrientes.

De ahí que en atención a la naturaleza de la actividad y de los riesgos que involucra o genera su ejercicio y el funcionamiento de los servicios que ofrece; el interés público que en ella existe; el profesionalismo exigido a la entidad y el provecho que de sus operaciones obtiene, los riesgos de pérdida por transacciones electrónicas corren por su cuenta, y por lo tanto, deben asumir las consecuencias derivadas de la materialización de esos riesgos a través de reparar los perjuicios causados, y no los usuarios que han confiado en la seguridad que les ofrecen los establecimientos bancarios en la custodia de sus dineros, cuya obligación es apenas la de mantener en reserva sus claves de acceso al portal transaccional.

Desde luego que consumada la defraudación, el Banco para exonerarse de responsabilidad, debe probar que esta ocurrió por culpa del cuentahabiente o de sus dependientes, que con su actuar dieron lugar al retiro de dinero de la cuenta, transferencias u otras operaciones que comprometieron sus recursos, pues amén de que es este quien tiene el control de mecanismo que le permiten hacer seguimiento informático a las operaciones a través de controles implantados en los software especializados con los que cuentan, la culpa incumbe demostrarla a quien la alegue (art. 835 C.Co.), pues se presume la buena fe aún la exenta de culpa.

3.4. EL CASO CONCRETO: Con fundamento en las consideraciones que preceden, esta judicatura abordará el caso concreto planteado.

Como se dejó dicho desde los reparos concretos a la decisión el cuestionamiento en que se funda la alzada tiene que ver con la valoración de los medios de convicción, en los cuales la falladora de primer grado determinó orfandad probatoria en cuanto a la culpa que alega la entidad demandada, debe ser asumida por el demandante, quien a su decir, desconoció la cautela con que debía salvaguardar sus claves y datos personales, para impedir la ocurrencia de los riesgos derivados de transferencias electrónicas, sin embargo, desde ahora se deja dicho que con el estudio del plenario y el recaudo probatorio documental que obra en la actuación, la tesis que se defenderá en sede de alzada, guarda simpatía con la conclusión a la que se arribó en primera sede y por consiguiente los reproches formulados por el apelante único, no encuentran prosperidad, conforme las razones que pasan a exponerse.

En primera medida y por ser el argumento reiterado al que acude el apelante en su defensa, relativo a que obra en el plenario la evidencia de que el Banco Av Villas cuenta con un sistema de prevención de fuga de la información llamado “Websense Content Portection suite” y en soluciones de transferencias de archivos con el programa “Secure Transport Tumbleweed” y actualización de software suscription”; programas que cuentan con la más alta tecnología del mercado que no sólo brindan seguridad en operaciones y transacciones, si no que cuentan con la mejor calidad del mercado, que proporcionan seguridad a los clientes para el manejo de transacciones y operaciones. Aun cuando se tuviera como cumplido dicho deber de cuidado y se asumiera que, en efecto, cuenta la entidad financiera con soporte tecnológico sólido que le permita atender situaciones de fraude, es un asunto que no alcanza la relevancia esperada, pues conforme con la jurisprudencia en cita, el alcance de la responsabilidad civil bancaria, se entiende derivada del ejercicio y del beneficio que reporta su especializada actividad financiera, a menos que logre acreditarse con prueba irrefutable culpa del cuenta habiente o de sus dependientes o representantes.

Implica lo anterior que, aún de haberse verificado la aplicación de extremas medidas de seguridad en el portal de la entidad financiera puesto a disposición de sus clientes para realizar operaciones de pago y transferencias a debitar de sus cuentas, de no establecerse la culpa en el usuario la carga reparadora seguiría incólume en cabeza de la entidad bancaria. Por ende, si se tuviera por sentada la suficiencia de las partidas destinadas por AV Villas para afrontar los peligros de ataques informáticos y suplantaciones en los equipos empleados para transacciones electrónicas, la sola ocurrencia del suceso no imputable a la falta de cuidado de la demandante en este caso era suficiente para asumir la carga reparadora, esto porque presupone la falta de rigor y proactividad para afrontar situaciones particulares y extraordinarias que atenten contra los recursos del público en general.

De suerte que, si la sustracción no fue el resultado de una actuación culposa del cliente, quiere decir que cualquiera pudo ser víctima, y era un deber inexcusable de la entidad financiera precaverlo. De todas maneras las razones que expone el recurrente, quien acude a las dos investigaciones internar realizadas en el banco, a propósito de la transacción fraudulenta perpetrada al demandante en el crédito rotativo y la cuenta de ahorros del demandante, con fecha del 15 de marzo de 2013, según las cuales no se logró detectar el movimiento engañoso pues los datos e información usados para su consumación correspondían a los del cliente – demandante, lo que hizo imperceptible alguna sospecha sobre dicho movimiento.

Sin embargo, comparte este Despacho la apreciación de la juzgadora de instancia, en el sentido de que si la cuenta del demandante había sido objeto de bloqueo en la misma fecha por presunción de operación fraudulenta y si al parecer fue concomitante el desbloqueo de la cuenta con la realización de la transacción, esa mera circunstancia debió alertar para verificar la ocurrencia de ese movimiento tramposo, máxime que al momento de corroborarse la realización de la transacción vía telefónica, manifestó el cliente al empleado del banco, que no había ejecutado ninguna operación financiera en ese momento. Esa circunstancia, también debió generar no sólo alerta, sino acciones concretas por parte del banco y de sus sistemas de seguridad para evitar, si no la realización de la transacción, por lo menos acciones posteriores que permitiera esclarecer lo ocurrido. Empero ello no fue así.

Dado el contexto en que se presenta la transacción financiera reprochada, resulta inverosímil desvirtuar la falta de asidero a las afirmaciones del Banco en relación con las seguridades que dice haber tomado y con que cuenta para impedir la ocurrencia de los riesgos propios de la actividad realizada por medios electrónicos, pues aun cuando pudiera asegurarse que lo sucedido se trata de un caso aislado o único, lo cierto es que esa tipo de situaciones debe ser detectados por la entidad financiera, pues ameritan las mismas medidas urgentes correctivas y preventivas para evitar su ocurrencia.

En Colombia, la Superintendencia Financiera a través de la Circular Básica Jurídica de 2014 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 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. Así mismo, 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.

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. Así, la doctrina ha definido el riesgo como la 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.

Ahora en materia de responsabilidad civil, la jurisprudencia ha reconocido las siguientes teorías de riesgo: riesgo provecho, riesgo creado, riesgo profesional; que 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. Sin embargo, no es posible predicar lo mismo del consumidor financiero, quien en ocasiones 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. En efecto, puede ser usual que los clientes consumidores financieros compartan las claves con personas que le son cercanas y ese hecho multiplique 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 asumidas por el consumidor y que de presentarse un fraude, como en efecto es el caso que se analiza, deben ser evaluadas por el operador jurídico al atribuir la responsabilidad.

Las consideraciones que preceden interesan en el presente análisis por cuanto, reclamó el extremo apelante que en sede de primera instancia no se valoró la información aportada en el interrogatorio de parte absuelto por la representante legal de la entidad bancaria, que consiste en un CD que contiene el historial de transacción del cliente – demandante, el extractos de su cuenta, el pantallazo de la transacción objeto de discusión, donde consta que esta fue ejecutada con la clave y usuario del cliente, tal y como arrojaron las investigaciones internas realizadas por la entidad bancaria y pantallazo del correo electrónico denominado “RE: Claves OTP JUAN FELIPE YASSER ESCOBAR” el cual contiene las claves OTP remitidas a los canales autorizados por el cliente, esto es, el celular y el correo electrónico; documentos que obran en la carpeta del cuaderno principal denominada “*ContenidoCDFolio55ExpedienteDigitalizado*”

Verificado el contenido de dichos medios de prueba, en el que sólo se constata información transaccional del cliente y sus extractos bancarios, no puede deducirse de su contenido que estemos ante evidencia de que la transacción verificada de forma fraudulenta fue producto de un descuido o actuar negligente del cuentahabiente. Si bien es cierto, la mentada transacción fue realizada con la habitualidad que el cliente acostumbra y dadas esas características el banco no encontró alerta alguna que pudiera significar un posible fraude o delito, ese argumento se queda sin piso ante la afirmación indeterminada de demandante acerca de la llamada recibida al momento en que se realizaba la operación bancaria, en la que informó que no se encontraba un ejecución de ninguna transacción por ese valor, máxime que estaba bajo el convencimiento que su cuenta se hallaba bloqueada, pues aunque no se tiene la prueba de dicha llamada por contar con el registro telefónico solicitado al ente accionado, en el interrogatorio de parte rendido por la representante legal del Banco no fue desacreditado ese hecho.

Los medios documentales aportados por la entidad bancaria, si bien dan cuenta de que la operación ejecutada podría ser una de aquellas que constituyen un monto de las operaciones diarias del demandante, esa circunstancia, en nada disminuye el grado de responsabilidad del Establecimiento Bancario. Pues aun cuando se brinde al cliente la facultad de fijar patrones en el manejo de sus cuentas que deben respetarse, quien en últimas debe tomar todas las precauciones para evitar sustracciones indebidas es el Banco por ser el guardián de los dineros, razón de suyo que explica el hecho de que deba asumir las pérdidas si el comportamiento del

titular o sus autorizados estuvo acorde con las directrices impartidas.

De suerte que, los elementos de convicción que se denuncian como mal apreciados, ya sea individualmente o en conjunto, no logran desvirtuar la conclusión a la que arribó la sentenciadora de primer grado, de que a pesar de existir métodos de protección a los consumidores del Sistema Financiero, estos eran insuficientes para blindarlos ante los riesgos cambiantes y exigentes de la cibernética, lo que por demás era intrascendente si las inconsistencias que se dieran en ese campo eran ajenas a actos culposos de aquellos.

Resulta entonces conclusivo que la carencia de pruebas sobre las aseveraciones respecto a la falta de cuidado y diligencia por parte de la demandante en el manejo de la clave, como único aspecto excluyente de responsabilidad bancaria en el asunto sometido a estudio, tampoco logra el dejar en evidencia la acusación en que se funda la apelación de la sentencia de primer grado.

En conclusión, la sentencia de primera instancia será confirmada íntegramente, incluso en lo que refiere a la condena en costas, y fundamento en el numeral 8 del artículo 365 CGP, en esta instancia no se impondrá condena en costas a la parte demandante, ante la no causación de las mismas.

Con fundamento en lo expuesto, **LA JUEZ VEINTIDÓS CIVIL DEL CIRCUITO DE MEDELLÍN**, administrando justicia en nombre de la república de Colombia y por autoridad de la ley,

FALLA:

PRIMERO: CONFIRMAR íntegramente la sentencia apelada, cuya naturaleza y procedencia se indicaron en la motivación.

SEGUNDO: SIN CONDENA EN COSTAS en esta instancia por no haberse causado las mismas (artículo 365 N° 8 del CGP).

TERCERO: En firme esta sentencia, devuélvase el expediente digital a su lugar de origen.

NOTIFÍQUESE Y CÚMPLASE

ADRIANA MILENA FUENTES GALVIS

Juez

LFG



Firmado Por:
Adriana Milena Fuentes Galvis
Juez Circuito
Juzgado De Circuito
Civil 022
Medellin - Antioquia

Este documento fue generado con firma electrónica y cuenta con plena validez jurídica,
conforme a lo dispuesto en la Ley 527/99 y el decreto reglamentario 2364/12

Código de verificación: **3fda91b8864fe750a8d70ce18abae624d8b7b315fb53d1c6b947293d7c73dabe**

Documento generado en 14/12/2023 01:03:41 PM

Descargue el archivo y valide éste documento electrónico en la siguiente URL:
<https://procesojudicial.ramajudicial.gov.co/FirmaElectronica>