República de Colombia
Corte Suprema de Justicia
Sala de Casación Civil

ARIEL SALAZAR RAMÍREZ
Magistrado Ponente

SC18614-2016

Radicación n° 05001-31-03-001-2008-00312-01
(Aprobada en sesión de veintitrés de diciembre de dos mil dieciséis)

Bogotá D.C., diecinueve (19) de diciembre de dos mil dieciséis (2016)

Decide la Corte el recurso de casación interpuesto por la parte demandada contra la sentencia de veinte de julio de dos mil trece, proferida por la Sala Civil del Tribunal Superior del Distrito Judicial de Medellín dentro del proceso ordinario de la referencia.

I. ANTECEDENTES

A. La pretensión

Tax Individual S.A. solicitó declarar contractualmente responsable al Banco AV Villas por la sustracción no

autorizada de $124'590.000 de su cuenta de ahorros, suma que debe reembolsarle con intereses comerciales desde el veintitrés de noviembre de dos mil siete o debidamente indexada.

En subsidio, por vía extracontractual, formuló idénticas peticiones indemnizatorias.

B. Los hechos

1. En el año dos mil dos, la demandante abrió la cuenta de ahorros No. 515021988 en el Banco Comercial AV Villas S.A., entidad que desde esa época puso a su disposición el portal de internet y red informática para realizar operaciones de recaudo de cartera, pago a proveedores y consulta de saldos.

2. Por la utilización de dichos canales transaccionales, la actora debía pagar unos montos determinados, los cuales a la presentación de la demanda ascendían a $1.300 + IVA por recaudo y $2.753 + IVA por transferencia.

3. El acceso y uso de la red del establecimiento de crédito se realizaba bajo las condiciones y requisitos impuestos por este, a las cuales debió adherir la actora por la naturaleza de la relación contractual.

4. Las transacciones electrónicas siempre se efectuaron desde un computador de la oficina de contabilidad de la empresa, operado por los empleados Maryory Deossa Valderrama y Johan Mosquera Lozano.

5. Como actividad propia de sus funciones, la señora Deossa Valderrama, al inicio de su jornada, verificaba en el portal de internet del Banco, los saldos existentes en la cuenta de ahorros y los recaudos del día anterior.

6. El veintidós de noviembre de dos mil siete, al digitar el nombre completo de la entidad financiera para acceder a su página web, el portal reportó que no estaba disponible y que se restablecería el servicio en doce horas.

7. En virtud de lo anterior, la empleada de contabilidad Maryory Deossa salió de la página web sin ingresar a la cuenta de ahorros ni realizar consulta alguna.

8. A las 7:30 a.m. del día siguiente, ingresó nuevamente al portal para consultar la cuenta bancaria, encontrando un faltante de dinero, el cual posteriormente y a partir de la información suministrada por la misma página web, se conoció que había sido de $124'590.000.

9. Las investigaciones realizadas permitieron establecer que la sustracción se produjo durante el día veintidós de noviembre y la madrugada del veintitrés de noviembre de dos mil siete, mediante el traslado a once cuentas pertenecientes a clientes del mismo Banco por valores de $84'590.000 en la primera fecha y $40'000.000 en la segunda.

10. Tales hechos fueron puestos en conocimiento de AV Villas el mismo veintitrés de noviembre, y de la Fiscalía

General de la Nación.

11. El Banco inició la investigación correspondiente hasta el quince de enero de dos mil ocho, fecha en la que fueron inspeccionados los equipos y sistemas de computación de Tax Individual S.A.

12. El ingeniero encargado por el Banco para esa labor, le informó a la demandante que el fraude se realizó bajo la modalidad de «*phising* (sic) *o spoofing*», y los once destinatarios de las transferencias retiraron los dineros abonados a sus cuentas en sucursales de las ciudades de Barranquilla y Santa Marta.

13. Durante los cinco años de operación de la cuenta de ahorros, la demandante nunca efectuó transferencias desde direcciones IP diferentes a las de su sede, ni con destino a cuentas bancarias de las ciudades mencionadas, por lo que la situación reportada era anómala y pudo ser detectada y evitada por el Banco.

14. Aunque AV Villas S.A. conoció inmediatamente de la defraudación, no tomó ninguna medida, no la investigó de manera oportuna, no orientó a la demandante sobre el procedimiento que debía seguir, ni reintegró el dinero sustraído.

15. El banco está llamado a responder por el fraude, porque las transferencias no se realizaron desde la dirección IP de la empresa ni por un empleado suyo, y se

utilizó el portal de internet de la entidad, cuyo contenido y seguridad son dispuestos por esta.

16. La demandada nunca la instruyó sobre las medidas a adoptar para evitar defraudaciones mediante la modalidad empleada por los delincuentes, ni implementó las mínimas requeridas como el permitir operaciones desde una sola dirección IP, el certificado digital, la configuración de un VPN y mecanismos para detectar transacciones irregulares o anormales.

17. Tax Individual S.A. no incurrió en culpa; por el contrario, siempre obró con cautela; durante los cinco años de existencia de la cuenta, su manejo estuvo a cargo de los dos funcionarios mencionados, quienes accedían a la página web anotando la dirección del Banco en el navegador; además, de manera permanente contó con programas firewall, antivirus y antispam.

18. En el año dos mil siete, ocurrieron varias defraudaciones con anterioridad a la perpetrada contra la demandante, pero la entidad financiera no tomó medidas de seguridad en relación con su portal de internet, ni oportunamente impartió instrucciones a sus clientes para evitarlas, a pesar de que la financiera es una actividad peligrosa, en la que los servicios por vía electrónica incrementan el riesgo.

C. El trámite de la primera instancia

1. La demanda se admitió en auto de dieciséis de julio de dos mil ocho, en el cual se ordenó notificar a la parte demandada y correrle el traslado de rigor [Folio 107, c. 1].

2. AV Villas S.A. se opuso a las pretensiones de la demandante; admitió solo algunos de los hechos aducidos, y formuló excepciones de mérito que fundó en la ocurrencia de un ilícito penal, el incumplimiento de los deberes contractuales de la depositante, el hecho de un tercero, culpa de la víctima, ausencia de culpa del Banco, una eximente de responsabilidad pactada, falta de legitimación de AV Villas y de causa para pedir.

Como fundamento de tales defensas, señaló que no puede atribuírsele responsabilidad por un hecho delictivo que no cometió; el daño no proviene de la inejecución del contrato, sino del incumplimiento de la actora «*al no tener la suficiente diligencia y cuidado con sus claves*» que son de su exclusiva responsabilidad y no son conocidas por el Banco; la empresa Tax Individual S.A. permitía el acceso al servicio de internet de sesenta usuarios; la conducta lesiva fue realizada por un tercero a quien debió demandarse y la entidad no incurrió en falta alguna, ni obró de manera negligente, ha realizado grandes inversiones y contratado la tecnología necesaria para brindar seguridad en las operaciones electrónicas, habiéndose eximido de responsabilidad por estas en el reglamento de convenios para la prestación de servicios bancarios aceptado por la

depositante [Folios 141-145, c. 1].

3. La juez *a quo* accedió a las pretensiones de la sociedad; en consecuencia, condenó a la parte demandada al pago de $124'590.000 más intereses desde el veinticuatro de noviembre de dos mil siete hasta su satisfacción [Folio 25, c. 1].

Lo anterior con fundamento en que la sustracción de dineros se produjo a través del portal de internet del Banco AV Villas, sin que con las pruebas recaudadas se hubiera demostrado la omisión o conducta imprudente de la demandante que posibilitó las transacciones fraudulentas.

Además, la empresa reclamante acreditó la existencia del daño y del nexo causal que le correspondía probar conforme a la teoría del riesgo creado, y aun si no se aceptara ésta, lo cierto es que de las afirmaciones del Banco se infiere que no adoptó las medidas necesarias para evitar el fraude, ni instruyó a la actora en la realización segura de transacciones en internet, atendiendo el alto volumen de operaciones y de dinero involucrados en la cuenta empresarial, siendo, por último, ineficaz, la cláusula de exoneración impuesta por el Banco a través de sus reglamentos [Folios 21-24, c. 1].

4. Inconforme con lo resuelto, AV Villas S.A. interpuso el recurso de apelación [Folio 234, c. 1].

D. La providencia impugnada

El Tribunal, en fallo proferido el treinta de julio de dos mil trece, confirmó la determinación adoptada por la juzgadora de primera instancia.

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

La responsabilidad de esas instituciones cesa si por culpa del cuentahabiente, sus dependientes o representantes, se produce un pago o se perfecciona un traslado en virtud de fraude, firmas falsificadas o alteradas, *«situaciones que no se consolidan tratándose de transacciones realizadas por internet por su misma dinámica que difiere de la materialidad»*, donde el usuario solo se compromete a *«conservar en reserva la clave y cuidar la tarjeta que le permite el acceso a ese medio, mientras que la entidad bancaria continúa siendo la garante y custodio de los dineros que en depósito se le han entregado»*.[1]

---

1 Folio 81 reverso, c. Tribunal.

Sin embargo, los testimonios referidos por el apelante no demuestran que la parte demandada hubiera cumplido «*con la obligación que se le exige, por la actividad profesional y especializada que ejerce, de brindar mayor seguridad en el uso de los servicios que ofrece*», la cual «*es especial cuando de medios electrónicos se trata*».

Por ejemplo, no implementó el uso del dispositivo denominado «*token*», el cual «*genera una serie de números que varía constantemente, u otras opciones como conexiones VPN, transacciones desde una única IP de TAX INDIVIDUAL*», sin que sea posible para un usuario normal identificar el engaño cometido bajo la modalidad de «*phishing*», a menos que cuente con la capacitación requerida, la cual no fue proporcionada por la entidad bancaria.[2]

Es evidente la ausencia de prueba de la falta de cuidado y diligencia de la demandante en el manejo de la clave, y de las seguridades tomadas por el Banco para evitar que acaecieran los riesgos de fraude informático, los cuales no pueden ser trasladados al usuario, sino que por estos «*debe responder la entidad financiera, dada la actividad profesional a la cual se dedica, lo que le exige para enfrentar los problemas que presenta el servicio que ofrece la utilización de medios de seguridad actualizados y apropiados...*».

Lo anterior desemboca en responsabilidad «por el hecho de haber atendido transacciones de forma irregular,

---

2 Folios 82 y 83.

sin que correspondieran verdaderamente a la orden dada por sus clientes».3

I. LA DEMANDA DE CASACIÓN

Se plantea un solo ataque por la vía indirecta de la causal primera del artículo 368 del Código de Procedimiento Civil, como consecuencia de yerros de facto cometidos en la valoración probatoria.

CARGO ÚNICO

Acusa la violación de los artículos 1494, 1602, 1603, 1604, 1608, 1613, 1614, 1615, 1617, 1757, 2341 y 2357 del Código Civil; 731, 732, 822, 871, 1382, 1391, 1396 y 1398 del de Comercio; 2,10, 11 y 15 de la Ley 527 de 1999; y 72 y 98 numeral 4 del Decreto 663 de 1993, el primero modificado por el 12 de la Ley 795 de 2003 y el último derogado en lo que se refiere a los numerales 4.1, 4.2, 4.3, 4.4 y 5 por el 101 de la Ley 1328 de 2009.

Lo anterior por cuanto el sentenciador de la segunda instancia dio por probado, sin estarlo, que:

(i) Faltó cuidado y la implementación de medidas de seguridad en los servicios de banca electrónica,

(ii) La demandante fue diligente en el manejo de las transacciones realizadas por medios electrónicos.

---

3 Folios 83 reverso y 84.

(iii) El Banco incurrió en responsabilidad civil contractual por incumplimiento del contrato de cuenta de ahorros que celebró con Tax Individual S.A.

(iv) Dicha empresa sufrió perjuicios patrimoniales por haber atendido la demandada, unas transacciones que no correspondían a órdenes impartidas por el cliente.

El Tribunal -sostuvo el censor- soslayó que en el expediente no obra prueba de que la página web de la entidad se hubiera adulterado o manipulado por terceros, ni mucho menos que las transacciones espurias se presentaron por ausencia de controles, ni de que el manejo de la cuenta de ahorros por su titular fue el adecuado.

Se menospreciaron los siguientes medios probatorios:

a) Los testimonios de Carlos Alberto Botero Vélez y José Isaías Gracia Rodríguez que dan cuenta de los «*altos estándares de seguridad tecnológica*» para la fecha de los sucesos.

b) La certificación expedida por el Gerente de Contabilidad del Banco, a la cual se anexan cinco facturas cambiarias de compraventa libradas por Etek International Holding Corp. Sucursal Colombia, las cuales se relacionan con la compra de servidor, software y renovación de servicios de seguridad informática para salvaguardar la información de los clientes.

c) Las condiciones autorizadas por Tax Individual S.A. para el uso del portal de internet, donde figuran los límites máximos de $100'000.000 diarios y por transacción, sin indicar otras restricciones.

d) Los documentos donde consta que antes de expedirse la Circular 052 de 2007 de la Superintendencia Financiera, los sistemas de AV Villas permitían dejar constancia de «*la dirección IP desde la cual se hizo la operación realizada por Internet, número de la operación, cuenta (s), montos, usuarios, etc*»[4], como demostración del elevado nivel de seguridad tecnológica.

e) La confesión en el hecho séptimo de la demanda «*del alto grado de diligencia y seguridad del Banco en el manejo de su servicio a través del portal de internet*», que a la depositante no le mereció reparos durante más de 5 años, en que no se reportaron anomalías, a pesar de «*las miles de operaciones de recaudo y las transferencias electrónicas*»[5] llevadas a cabo.

f) El memorando interno del Banco de veintidós de enero de dos mil ocho, que envió el Gerente de Seguridad al Gerente de Riesgos, donde se precisa que el 22 de Noviembre de 2007, la contadora de la demandante no entró a la página web de la entidad, sino a la dirección electrónica *http://www.avvillas.com.co/transac-bbs*», en la que el «*hipertexto "http" carece de la "s"*» y así lo corroboró el

---

4 Folio 40.
5 Folio 42.

testigo José Isaías Gracia Rodríguez, lo que identifica que no correspondía a la dirección del portal transaccional de AV Villas.

Es inaudito -añadió- que el juzgador hubiera apoyado su determinación en el pronunciamiento de la Sala de Casación Civil de dieciséis de junio de dos mil ocho, relacionado con el pago de un cheque con firma falsificada, y en los artículos 732, 733 y 1391 del Código de Comercio, cuando se refieren a supuestos fácticos diferentes. Además, citó como vigente el numeral 4° del artículo 98 del Estatuto Orgánico del Sistema Financiero que está derogado.

Incurrió así en un «*claro y evidente error de hecho en la contemplación de la demanda*», y por otra parte, desconoció el siguiente material probatorio a partir del cual se establecía la culpa del consumidor financiero:

a) La denuncia penal instaurada por Tax Individual S.A., donde quedó claro que el Banco no tuvo responsabilidad en los hechos, pues o bien la culpa es atribuible a dicha empresa porque su contadora ingresó a una página web falsa y digitó la clave de acceso que sólo ella conocía, o el daño fue el producto del dolo de terceros, fallando en ambos casos el deber de custodia y vigilancia de la titular de la cuenta.

b) Los testimonios de Maryory Deossa Valderrama, contadora de la demandante y Johan Mosquera Lozano, el otro funcionario que contaba con clave de acceso a la

cuenta de ahorros, con los cuales se demuestra que el proceder de la primera fue «*negligente, descuidado y totalmente fuera de lo acostumbrado para el manejo de una cuenta*»[6] al no darle trascendencia al aviso de problemas en la página web, cuando debió llamar inmediatamente a la entidad para averiguar si eran reales; ejercer control con el funcionario que manejaba la otra clave, o consultarle al ingeniero de sistemas de la empresa.

c) El memorando de 22 de enero de 2008 y las declaraciones de José Isaías Gracia Rodríguez y Yeison Ferney Arias Castrillón, relacionadas con el inusual pantallazo de deficiencias técnicas que no provino de AV Villas, pues, la dirección *http* era disímil de la usual, y la omisión de la encargada de contabilidad, de poner al tanto de la situación al personal de apoyo o al Banco, lo que facilitó la conducta de los delincuentes.

d) El registro de las transacciones realizadas entre el treinta de junio de dos mil cinco y el veintitrés de noviembre de dos mil siete, en el que aparecen las que se hicieron el veintidós de noviembre de dos mil siete desde las 15:06:21 hasta las 19:06:22 horas, esto es durante el lapso en el que la empleada guardó silencio.

e) El testimonio de Javier Andrés Arango Salazar, del cual el Tribunal dedujo que «*a las claras permite ver que el Banco carecía de medidas de seguridad para los servicios*

---

6 Folio 45.

ofrecidos a través de su portal de internet», en realidad no era indicativo de tales falencias, ya que sus observaciones sobre la fragilidad para acceder al portal de internet del Banco no provienen de «*una peritación a los sistemas y esquemas de seguridad y calidad que maneja el Banco AV Villas, ni a sus protocolos, servicios, aplicaciones, usuarios, equipos, contratos con terceros proveedores de servicios, controles, seguridades, funcionamiento, pruebas etc.*»[7]; el declarante fue consultor en informática de la demandante y era ésta la que personalizaba las condiciones de acceso a la página web.

De no haber incurrido el sentenciador en los yerros mencionados -aseveró el casacionista-, hubiera concluido que el Banco no estaba llamado a indemnizar a la reclamante por el fraude del que fue objeto. En consecuencia, debe casarse la providencia impugnada, y en sede de instancia, absolverlo de las pretensiones elevadas en su contra.

CONSIDERACIONES

1. Es indiscutible la trascendencia de la actividad financiera en la economía, tan es así 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*

---

7 Folio 50.

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, señala como integrantes de éste a los establecimientos de crédito, de los cuales hacen parte los establecimientos bancarios, que en el artículo 2° 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*».

Se trata de un mercado de intermediación entre los ahorradores y los prestatarios potenciales, los primeros en pos de resguardar su capital y obtener una rentabilidad, y los otros con el fin de conseguir recursos para atender proyectos que retornarán aumentados con intereses.

1.1. 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 *ibidem*.

En ese sentido, esta Corporación 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).

De ahí que entre las reglas de competencia y protección al usuario se fijara a las instituciones del sector, según la redacción inicial del artículo 98 ordinal cuarto *id*), el deber de «*emplear la debida diligencia en la prestación de los servicios a sus clientes a fin de que éstos reciban la atención debida en el desarrollo de las relaciones contractuales que se establezcan con aquellas y, en general, en el desenvolvimiento normal de sus operaciones*», así como la prohibición de «*convenir cláusulas que por su carácter exorbitante puedan afectar el equilibrio del contrato o dar lugar a un abuso de posición dominante*» (se destaca).

A pesar de que la Ley 795 de 2003, en su artículo 24, introdujo una modificación a dicho ordinal, se conservó la esencia de la norma original en el numeral 4.1, pero con los numerales 4.2 al 4.4 fue institucionalizada la figura del Defensor del Cliente como vocero de los usuarios frente al establecimiento; la fijación de procedimientos para el conocimiento de quejas, y contemplar sanciones por el incumplimiento de las obligaciones que de allí se derivan.

Y si bien el artículo 101 de la Ley 1328 de 2009 derogó expresamente «*los numerales 4.1, 4.2, 4.3, 4.4 y 5 del artículo 98 del Estatuto Orgánico del Sistema Financiero*», precisó que la pérdida de vigencia operaría «*a partir del 1° de julio de 2010*», esto es, con mucha posterioridad a la ocurrencia de los hechos y al comienzo del litigio, por lo que cualquier análisis del caso se regía por el anterior precepto.

De todas maneras, no se puede pasar por alto que la razón de ser de la derogatoria fue que en la Ley 1328 de 2009, se desarrolló lo concerniente al Régimen de Protección del Consumidor Financiero, con el propósito de «*establecer los principios y reglas que rigen la protección de los consumidores financieros en las relaciones entre estos y las entidades vigiladas por la Superintendencia Financiera de Colombia, sin perjuicio de otras disposiciones que contemplen medidas e instrumentos especiales de protección*» (art. 1).

Incluso se delimitaron como principios orientadores de las relaciones entre los consumidores financieros y las entidades vigiladas, la «*debida diligencia*» de éstas al ofrecer los productos o prestar los servicios entregando la información y atención debida «*en el desenvolvimiento normal de sus operaciones*», fuera de la «*transparencia e información cierta, suficiente y oportuna*» que le permita a aquellos conocer sus derechos, obligaciones y costos del vínculo (art. 3°, literales a y c).

1.2. 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*».[8]

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 *id.*).

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

---

8 BARBIER, Eduardo Antonio. Contratación Bancaria, Tomo I, Consumidores y usuarios, Buenos Aires: Editorial Astrea, 2° Edición, 2002, pág. 42.

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.

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

2.1. *La Ley "sobre instrumentos negociables"* y la teoría del riesgo creado:

Establecía el artículo 191 de la Ley 46 de 1923, que «*Todo Banco será responsable a un depositante por el pago que aquél haga de un cheque falso o cuya cantidad se haya aumentado, salvo que dicho depositante no notifique al banco, dentro de un año después de que se le devuelva el comprobante de tal pago, que el cheque así pagado era falso o que la cantidad de él se había aumentado*» (se destaca).

Conforme a esta disposición, la responsabilidad de los bancos por el pago de cheques falsificados o cuyo importe había sido incrementado, era casi absoluta, pues su exoneración estaba supeditada a que el cuentacorrentista dejara pasar el término allí previsto sin darle aviso de la

falsedad del título o del incremento de su valor, de modo que el régimen se caracterizaba por ser manifiestamente protector de los clientes.

La jurisprudencia de esta Sala entendió que dicho precepto deducía la responsabilidad del Banco bajo la teoría del riesgo creado (CSJ SC, 9 Dic. 1936, G.J. T. XLIV, 405, reiterada en CSJ SC, 15 Jul. 1938, G. J. T. XLVII, 68, y CSJ SC, 11 Mar. 1943, G. J. T. LV, 48).

En el esquema de la mencionada formulación, se prescinde del análisis de la culpa como elemento para atribuir aquella y siendo una manifestación de responsabilidad objetiva, algunos consideran que se basa en la «*inobservancia de normas de cautela, antes que en una valoración del actuar de la persona y de sus perfiles subjetivos*»9, de ahí que no se recurra a la culpabilidad como criterio de imputación.

También se ha sostenido que «*La teoría del riesgo, impregnada por el valor moral de la solidaridad, parece sobre todo inspirada por la equidad: Por su actividad, el hombre puede procurarse un beneficio (o, al menos, un placer). Es justo (equitativo) que en contrapartida él repare los daños que ella provoca. Ubi emolumentum, ibi onus (ahí donde está la ventaja, debe estar la carga).*10

Su fundamento, según los autores precitados, resulta «*del poder que tenía el responsable de evitar el daño. O para decirlo de otra manera por vía de una expresión a la cual nosotros adherimos y que empleamos usualmente, en su*

9 DÍEZ-PICAZO, Luis. Derecho de Daños, Madrid: Civitas, 1999.

10 TRIGO REPRESAS, Félix A. y LÓPEZ MESA, Marcelo J. Tratado de la responsabilidad civil. Tomo IV. Buenos Aires: La Ley. 2004, p. 931.

dominio; dominio que él tenía o, al menos, habría debido normalmente tener, de su actividad, así como de los hombres o de las cosas por las que él responde».[11]

Sobre su aplicación a la actividad de los Bancos, esta Corporación sostuvo lo siguiente:

> (...) *al Banco correspondía soportar las consecuencias derivadas del pago de un cheque falsificado o cuya cantidad se hubiera aumentado, responsabilidad de la cual no se exoneraba ni aún con la prueba de que la falsedad o la adulteración habían encontrado su causa determinante en la conducta negligente del cuentacorrentista, en la guarda del instrumento. Los perjuicios de dicho cobro indebido eran, pues, de cuenta del Banco girado, siempre que el cliente le hiciera saber oportunamente el hecho fraudulento* (CSJ SC, 9 Sep. 1999, Rad. 5005; se subrayó).

2.2. *La posición de la jurisprudencia frente a la previsión de la Ley 46 de 1923:*

Al poco tiempo de expedirse la Ley de instrumentos negociables, esta Corporación comenzó a precisar en relación con los estrictos términos del artículo 191, que a pesar de que la responsabilidad por el pago de cheques falsos o adulterados recaía sobre las entidades bancarias y por eso el cliente no tenía la carga de probar el proceder culposo de la institución, aquella podía aminorarse o excluirse por causa de la culpa del cuentacorrentista.

---

11 Ibídem.

En ese sentido, haciendo referencia a que dicha regulación reproduce la imperante en ese momento en las legislaciones inglesa y estadounidense, explicó que «*los principios generales de la legislación civil no son los que inspiran la ley de instrumentos negociables*», y conforme a dichos principios, el sistema de «riesgo creado» que consagró «*no impide que el banco pueda exonerarse de responsabilidad demostrando una culpa, malicia, negligencia o imprudencia de parte del girador o de sus empleados. Sólo que la carga de la prueba de esas circunstancias corresponde darla al Banco*» (CSJ SC, 9 Dic. 1936, G.J. T. XLIV, 405).

Y después precisó:

> *Como la medida de la responsabilidad de un banco por el pago de un cheque falso no se detiene en la culpa sino que alcanza el riesgo creado, no le basta el lleno de las precauciones habituales, sino que es preciso probar algún género de culpa en el titular de la cuenta corriente para que el banco quede libre* (G.J. 1943, p. 43).

La relación existente entre el cliente y la entidad bancaria -sostuvo la Corte- «*requiere el intercambio continuo de confianza entre el banco y sus depositantes, a tiempo en que determina la reciprocidad de esfuerzos en la tarea de evitar el daño que se desprende de la emisión de cheques falsos. Esto acentúa la trascendencia de la culpa del depositante descuidado en la guarda de la chequera que el banco le suministrara para ser empleada como instrumento primordial de seguridad y control que le permita asumir precisamente el riesgo de empresa que le*

impone la ley a través de la presunción de responsabilidad por el pago de cheques adulterados. De donde habrá razón liberatoria de esa presunta responsabilidad, cuando la causa originaria del fraude inaparente cometido por tercera persona obedezca al notorio error de conducta en que el depositante haya incurrido en la guarda de su chequera. O sea, cuando por su apariencia el cheque discutido se presentó al pago completo y regular en su forma exterior, sin señales visibles de adulteración y dentro de la serie correspondiente al talonario que el Banco puso en manos de su depositante» (CSJ SC, 26 Nov. 1965, G. J., T. CXIV, 205 y 206).

2.3. El régimen de responsabilidad por el pago de cheques falsos en el Código de Comercio y la "responsabilidad de empresa":

Como el artículo 191 de la Ley 46 de 1923 no permitía la exoneración de las entidades bancarias aunque la conducta del depositante hubiera sido la causa de la falsedad o adulteración del título valor, el Decreto 410 de 1974 por el cual se expidió el Código de Comercio, estableció al artículo 1391 lo siguiente:

> *Todo Banco es responsable con el cuentacorrentista por el pago que haga de un cheque falso o cuya cantidad se haya alterado, salvo que el cuentacorrentista haya dado lugar a ello por su culpa o la de sus causahabientes, factores o representantes.*
>
> *La responsabilidad del banco cesará si el cuentacorrentista no le hubiere notificado sobre la falsedad o adulteración del cheque, dentro de los seis meses siguientes a la fecha en que se le envió la información sobre tal pago.*

Dicha disposición está en concordancia con lo estatuido por el artículo 732 de la misma codificación conforme al cual «*Todo banco será responsable a un depositante por el pago que aquel haga de un cheque falso o cuya cantidad se haya aumentado, salvo que dicho depositante no notifique al banco, dentro de los tres meses después de que se le devuelva el cheque, que el título era falso o que la cantidad de él se había aumentado.*

Si la falsedad o alteración se debiere a culpa del librador, el banco quedará exonerado de responsabilidad».

Aunque a simple vista, las dos normas mencionadas parecen entrar en contradicción, porque consagran lapsos diferentes para que el cuentacorrentista informe al Banco sobre la falsificación o adulteración del cheque, tal como lo ha precisado la jurisprudencia, esa dificultad se supera acudiendo al artículo 5° de la Ley 57 de 1887, el cual llevará a concluir que en cuanto a dicho término, el precepto aplicable es el 1391 «*por ser norma posterior al artículo 732 ib. y hacer parte de la normatividad que regula el contrato de cuenta corriente*» (CSJ SC, 9 Sep. 1999, Rad. 5005).

Posteriormente, en referencia a la previsión del citado artículo 1391, esta Corporación explicó que el riesgo de los cheques falsificados fue impuesto por la ley «*a las entidades financieras quienes, dado el volumen de transacciones que realizan, compensan las pérdidas que los cheques falsificados pueden causar, regla esta que, de acuerdo con las disposiciones recién aludidas, tiene como obvia excepción que la culpa de los*

hechos recaiga en el cuentacorrentista o en sus dependientes, factores o representantes» (se subrayó).

Y agregó:

(...) *según esta línea de pensamiento que hoy en día encuentra visible reflejo en el artículo 1391 del Código de Comercio, se estima que el ejercicio de la banca de depósito se equipara fundamentalmente al de una empresa comercial que, masivamente, atrae a sí y asume los riesgos inherentes a la organización y ejecución del servicio de caja,* ***luego es en virtud de este principio de la responsabilidad de empresa****, cuyos rasgos objetivos no pueden pasar desapercibidos, que el establecimiento bancario asumiendo una prestación tácita de garantía, responde por el pago de cheques objeto de falsificación, ello en el entendido, se repite, que es inherente a la circulación y uso de títulos bancarios de esta índole el peligro de falsificación y el costo económico de tener que pagarlos se compensa sin duda con el lucro que para los bancos reporta el cúmulo de operaciones que en este ámbito llevan a cabo. Pero, asimismo, no deben perderse de vista otros postulados acogidos sin reparo para atemperar el rigor de esta doctrina, habida cuenta que en cuanto ella hace pesar sobre el banco en su calidad de librado, el riesgo de "falsificación" a base de imputarle responsabilidad objetiva, lo cierto es que esta responsabilidad puede moderarse, e incluso quedar eliminada si corre culpa imputable al titular de la cuenta corriente*... (CSJ SC, 24 Oct. 1994, Rad. 4311; el énfasis es propio).

La obligación del Banco de resarcir los perjuicios ocasionados al cuentacorrentista con el pago de cheques espurios surgía, según lo expuesto, del *«principio de responsabilidad de empresa»*, en virtud del cual es a la entidad que desarrolla la actividad empresarial a la que le corresponde asumir las contingencias o riesgos que acarrea su operación, entre los cuales está el pago de cheques cuya falsificación no pueda imputarse al librador, no solo por cuanto son inherentes a aquella, sino porque se trata de una actividad realizada bajo su control y de la cual obtiene beneficio, razón por la cual al cliente no se le exige demostrar la culpa de la entidad, pues el legislador, a efectos de imponer que aquella debía asumir el riesgo, no reparó en su obrar, de ahí que si había sido diligente o culposo no era una cuestión relevante.

Esta Corporación puntualizó que la responsabilidad civil de la entidad financiera *«deriva del ejercicio y del beneficio que reporta de su especializada actividad financiera, como así lo tiene definido la jurisprudencia cuando asevera que una entidad crediticia es una empresa comercial que dado el movimiento masivo de operaciones, "asume los riegos inherentes a la organización y ejecución del servicio de caja"»* (CSJ SC, 24 Oct. 1994).

Y como contrapartida de su actividad empresarial *«el ordenamiento le atribuye* (al banco), *en inobjetable aplicación del principio "ubi emolumentum, ibi incomoda", la obligación de soportar tal contingencia* (el riesgo de pagar cheques falsos o adulterados), *imposición que, de todas formas, encuentra*

justificación igualmente válida en otros argumentos tales como que la falsedad se dirige y consuma contra el banco, pues, a la postre, el pago del cheque se produce con su propio dinero y no con el del cuentacorrentista, dada la particular naturaleza del depósito bancario. Empero, como ha quedado dicho, la responsabilidad bancaria en tal hipótesis no es absoluta, habida cuenta que ésta cesa, cuando la culpa de los hechos recaiga en el cuentacorrentista o en sus dependientes, factores o representantes» (CSJ SC, 9 Sep. 1999, Rad. 5005; CSJ SC, 11 Jul. 2001, Rad. 6201; CSJ SC, 31 Jul. 2001, Rad. 5831; se subrayó), lo que reclama la existencia de una relación de causalidad entre la culpa del librador o de las personas por las cuales responde y la falsificación o adulteración del instrumento cambiario.

Se trata -sostuvo la Sala- de «*una responsabilidad objetiva, que se modera o elimina en los casos atrás mencionados* (culpa del titular de la cuenta por las hipótesis previstas en los arts. 733 y 1391)» (CSJ SC, 31 Jul. 2001, Rad. 5831).

La obligación de la entidad crediticia -dijo después la Sala- «*se nutre en la teoría de la responsabilidad profesional, pues es por imposición legal que la entidad girada debe correr con las contingencias que surgen del desempeño de sus tareas, y concretamente con la del pago de cheques alterados o falsificados*», y «*sólo la presencia de circunstancias excepcionales...permiten liberar a las entidades bancarias de su responsabilidad*» (CSJ SC-176, 17 Sep. 2002, Rad. 6434).

2.4. La responsabilidad del Banco por el pago de cheques, cuyos formularios extravió el cuentacorrentista:

De conformidad con el artículo 733 del estatuto mercantil, el propietario de una chequera «*que hubiere perdido uno o más formularios y no hubiere dado aviso oportunamente al banco, sólo podrá objetar el pago si la alteración o la falsificación fueren notorias*».

En atención a lo dispuesto en esta norma, la Sala indicó:

> *El riesgo de la falsificación del cheque lo sufre la entidad bancaria porque, como se dice, ésta debe pagar, en principio, los cheques emitidos por el librador. En cualquier evento eximente de responsabilidad, corresponde al banco demostrar la culpa del cuentacorrentista, en cuanto éste se ampara en una amplia suposición frente al deber de aquél de no pagar un cheque falso o adulterado.*

Y añadió:

> «*El hecho de la pérdida del formulario del titular de la chequera* -sostuvo la Corporación- *no descarga, por sí solo, la responsabilidad del banco. Este es un deber del dueño de la chequera que no puede comportar un grado de culpa suficiente para eximir a aquél del daño causado por el pago de un cheque falso. Para ampararse el banco en la situación derivada de la pérdida, tiene que demostrar que la falsificación no fue notoria. Esto supone, entonces, que la*

carga de la prueba corra por cuenta del banco, para desvirtuar así la responsabilidad que asume del pago hecho en cheque falso, si se acredita dentro del proceso esta circunstancia (CSJ SC, 30 Sep. 1986, G.J. T. CLXXXIV, p. 290; se destaca).

Bajo esta interpretación, la exoneración del Banco estaba supeditada a un supuesto: Que la falsedad del cheque no era notoria, pues no le bastaba con alegar que el cuentacorrentista había perdido el formulario de ese título valor.

Tal criterio fue modificado posteriormente por la Sala, que al respecto consideró que el artículo 733 del Código de Comercio imponía la necesidad de diferenciar el pago de cheques falsificados o adulterados cuando no ha habido pérdida por parte del dueño de la chequera, el cual es un riesgo propio de la operación bancaria, del que se realice de instrumentos también apócrifos, cuyos formatos había perdido el cuentacorrentista.

Lo anterior, por cuanto ese hecho tiene la aptitud de cambiar los efectos del pago que realiza el Banco del título valor espurio al sustraerlo del régimen de responsabilidad por el riesgo profesional derivado de la actividad financiera especializada y del lucro que esta le reporta, previsto en los artículos 732 y 1391 del Código de Comercio.

En ese sentido, esta Corporación sostuvo que «*sin importar cuál haya sido la conducta del cuentacorrentista en el*

cuidado del talonario, él será el llamado a soportar las secuelas de su pérdida, de suerte que el banco sólo asumirá el resultado del pago del cheque apócrifo previamente perdido por el cuentacorrentista si éste lo enteró tempestivamente del hecho de la pérdida, o si la falsedad es cuestión notoria», aclarando que «*para que la falsedad plasmada en el cheque previamente sustraído al cuentahabiente pueda catalogarse como notoria, requiere que aparezca de bulto a quien la aprecia, o que del examen normal del instrumento pueda colegirse su ocurrencia, sin tornarse necesario para establecerla observaciones detalladas o técnicas. Ante la presencia de adulteración semejante el banco responderá por el pago que haya hecho del título valor, independientemente de cualquier otra consideración, en especial, de si su cliente le dio o no aviso oportuno del extravío del formulario respectivo*» (CSJ SC, 8 Sep. 2003, Rad. 6909; el subrayado no es del texto).

En caso de que la falsificación o alteración no sea notoria, el establecimiento bancario solo estará llamado a responder si el titular de la cuenta corriente le dio aviso oportuno «*de la pérdida del formato de cheque*»; en tal caso, el cliente «*podrá ejercer la facultad de objetar el pago, como quiera que él traduciría incumplimiento de la revocación de la orden documentada en el cheque (artículo 724 Código de Comercio)*» (ibídem).

Si el cuentacorrentista extravió el instrumento, pero no dio aviso al Banco previo a su pago, «*es a él, y sólo a él, al que compete el cumplimiento de la carga de acreditar que el instrumento contenía una falsedad o alteración palpable*».

Tal posición fue reiterada posteriormente precisando que en el específico caso contemplado en el artículo 733 del Código de Comercio, es decir, cuando media la pérdida de uno o más formatos de cheques por el titular de la cuenta corriente, *«sin importar que la pérdida del instrumento haya sido culposa o no, se invierte la regla de la responsabilidad a cargo del librado que se adopta en las disposiciones anteriores, para imponérsela al cliente, en el entendido de que si ha recibido el talonario respectivo, sin ningún reparo, de traspapelar uno o más formularios, "... a él le será atribuible semejante desatención en su custodia»*, principio que *«se excepciona en los casos en que oportunamente entera al librado de ese hecho, para que se abstenga de efectuar el procedimiento de descargo, y pese a ello lo realiza, lo mismo que cuando el fraude es fácilmente apreciable, hipótesis en las que es el banco el que debe soportar las contingencias del pago»* (CSJ SC-123, 15 Jun. 2005, Rad. 1999-00444-01; en el mismo sentido CSJ SC-127, 29 Sep. 2006, Rad. 1992-20139-01 y CSJ SC-054, 16 Jun. 2008, Rad. 1995-01394-01).

En conclusión, cuando el pago del instrumento adulterado o falseado no se deba a la pérdida por parte del propietario de la chequera sino que este se produce dentro del riesgo propio de su circulación, el asunto se rige por la regla de responsabilidad contenida en el artículo 1391 del estatuto mercantil, acorde con la cual a la entidad financiera le corresponde demostrar la culpa del cuentacorrentista o de sus dependientes en virtud de la aplicación de la teoría del riesgo profesional por la *«responsabilidad de empresa»*.

En cambio, si el pago del título apócrifo fue precedido de su extravío por el cuentahabiente, la controversia es gobernada exclusivamente por la previsión contenida en el artículo 733 de la codificación comercial, el cual carga a éste con las consecuencias de la falta de cuidado en la custodia de los formatos, de ahí que el hecho de su pérdida le es atribuible, y en esa medida le corresponde asumir los efectos del pago que haga el Banco, sin importar cuál haya sido su conducta en el cuidado del talonario, salvo que oportunamente le hubiere avisado a la entidad sobre tal circunstancia o que la falsedad o adulteración fuera evidente o notoria.

Luego, al cliente le incumbe demostrar la notoriedad de la falsificación o alteración, o que, en caso de que la falsedad no sea evidente, le avisó a la entidad tal hecho antes de que procediera al pago, en ejercicio de su facultad de objetarlo conforme a lo estatuido por el artículo 724 *ejusdem*; por su parte, al Banco no le es exigible la carga de demostrar la culpa del titular de la cuenta en la pérdida.

3. Conclusión de lo expuesto hasta ahora es que el régimen de responsabilidad de los Bancos por la defraudación con el uso de instrumentos espurios para disponer de los fondos depositados en cuentas, se ha fundado en vertientes de la teoría del riesgo: En una primera época, la del «*riesgo creado*» en virtud de la cual quien en desarrollo de una actividad genere un peligro o contingencia, debe indemnizar los perjuicios que de aquel deriven para terceros, con independencia de si ha actuado

de manera diligente o culposa, o de si ha obtenido o un provecho; después se dio aplicación a la teoría del «*riesgo provecho*» que carga con la obligación resarcitoria a quien ejerza la actividad que genera un riesgo o peligro y, además, saca de la misma una utilidad o percibe lucro, sin que importe que su conducta haya sido diligente o imprudente; por último, se acudió a la teoría del «*riesgo profesional*» que es una derivación de la anterior, empleada también en otras áreas del derecho como, por ejemplo, en materia de accidentes y enfermedades laborales. En esta última, la obligación de asumir los riesgos inherentes al ejercicio de la actividad se basa en el profesionalismo que esta requiere.

Sobre el origen de los anteriores postulados, esta Sala explicó:

> *A fines del Siglo XIX, surgen las doctrinas del "riesgo profesional" (risque professionnel, Raymond SALEILLES [1855-1912]), "riesgo creado" (risque créé, Louis JOSERRAND [1868-1941]), "riesgo beneficio", "riesgo de empresa" y postula la responsabilidad, no por culpa, sino por la asunción de una empresa o una actividad riesgosa en contraprestación al beneficio que de ella se recibe (ubi emolumentum ibi onus o ubi commoda ibi et incommoda o cuius commoda eius incommoda esse debet), bien por equidad, en tanto, el deber surgiría ex lege para quien genera el riesgo, dispone de una cosa, ejerce su gobierno o tiene su control»* (CSJ SC, 24 Ago. 2009, Rad. 2001-01054-01).

3. *La responsabilidad bancaria por fraudes con instrumentos diferentes a cheques:*

El régimen de responsabilidad de los Bancos que hasta ahora se ha descrito, deriva de las previsiones contenidas en los artículos 732, 733 y 1391 del Código de Comercio, ninguna de las cuales contempló los fraudes cometidos con instrumentos diferentes de los cheques u otros mecanismos a través de los cuales sea posible realizar la disposición de los fondos puestos por los ahorradores bajo la custodia y cuidado de tales entidades, tales como notas débito, certificados de depósito a término, transferencias y otras transacciones que involucren los recursos provenientes del ahorro privado.

Tal circunstancia, sin embargo, no conlleva la inaplicabilidad del régimen de responsabilidad reconocido por ellas a otra clase de defraudaciones cometidas tanto en la disposición irregular de recursos pecuniarios en cuentas corrientes como en las de ahorro, pues lo que subyace en la regulación mencionada es que el ordenamiento positivo reconoce que las instituciones bancarias ejercen una actividad que es profesional, habitual y de la que deriva un provecho económico, a la que le es inherente una multiplicidad de peligros, y entre ellos se encuentran los derivados de las operaciones que realizan (riesgos operacionales), que pueden afectar los intereses de los cuentahabientes por la mala disposición de sus depósitos.

Siendo la bancaria y la de intermediación financiera, actividades en las que -como atrás se dijo- existe un interés público y son realizadas por expertos que asumen un deber de custodia de dineros ajenos, siéndole exigibles, según lo previsto por el Estatuto Orgánico del Sistema Financiero (Decreto 663 de 1993) y las Circulares Básica Contable y Financiera (100 de 1995) y Básica Jurídica (007 de 1996) unos altos y especiales cargas o cumplimiento de estándares de seguridad[12], diligencia, implementación de mecanismos de control y verificación de las transacciones e incluso de seguridad de la confiabilidad de la información y preservación de la confiabilidad, es natural que la asunción de tales riesgos no les corresponda a los clientes que han encomendado el cuidado de parte de su patrimonio a tales profesionales, de ahí que sea ellos quienes deban asumir las consecuencias derivadas de la materialización de esos riesgos.

En ese orden de ideas, *«a la hora de apreciar la conducta de uno de tales establecimientos* -ha dicho la Corte- *es necesario tener presente que se trata de un comerciante experto en la intermediación financiera, como que es su oficio, que maneja recursos ajenos con fines lucrativos y en el que se encuentra depositada la confianza colectiva»* (CSJ SC-076, 3 Ago. 2004, Rad. 7447) y por tales razones se le exige *«obrar de manera cuidadosa, diligente y oportuna en ejercicio de sus conocimientos profesionales y especializados en materia bancaria»* para

12 Entre ellos la NTC-ISO/IEC 27001 aprobada el 22 de marzo de 2006, que recopila los requisitos exigidos para la implementación, revisión, mantenimiento y mejora del sistema de gestión de la seguridad de la información a fin de *«asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas»*

impedir que sean quebrantados los derechos patrimoniales de titulares de las cuentas de ahorro y corrientes de cuya apertura y manejo se encarga (CSJ SC, 3 Feb. 2009, Rad. 2003-00282-01).

De todo lo anterior deriva, necesariamente que en la materia impera un *«modelo particular de responsabilidad profesional del banco»* (CSJ SC-201, 15 Dic. 2006, Rad. 2002-00025-01).

Por eso, si *«entre las obligaciones que al banco impone el artículo 1382 del Código de Comercio, derivadas del contrato de cuenta corriente, "está la de mantener los dineros depositados regularmente para entregarlos en la medida que el cuentacorrentista haga disposición de ellos de acuerdo con las distintas modalidades reconocidas por la ley, por el contrato o por las prácticas bancarias. (...) Ante esos compromisos, el banco debe mantener las precauciones, diligencias y cuidados indispensables para que los actos de movimiento de la cuenta del usuario se alcance con plena normalidad; por eso,* ***cualquier desviación constituye un factor de desatención del contrato, dado su particular designio****"; de modo que "si llega a producirse una operación de transferencia de fondos que incida en el saldo, cualquier reclamo o inconformidad que muestre el cuentacorrentista puede comprometer la responsabilidad de la entidad bancaria que para exonerarse debe acreditar, por cualquier medio idóneo, que contó con la autorización de aquel" (sent. del 23 de agosto de 1988, resaltado fuera del texto)»* (ibídem)» (*ibídem*)..

Y lo mismo ocurre tratándose de cuentas de ahorro, porque en ellas el Banco «*es responsable por el reembolso de sumas depositadas que haga a persona distinta del titular de la cuenta o de su mandatario*» (art. 1398 C. Co.). Claro está, sin desconocer, en ninguno de los dos casos, que la responsabilidad de dicha institución financiera, puede atenuarse, moderarse e incluso excluirse en virtud de culpa atribuible al titular de la cuenta.

4. Las nuevas tecnologías y el riesgo de la actividad bancaria:

4.1. 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, recientemente, 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.

4.2. 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...*».[13]

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

13 PÉREZ LUÑO, Antonio Enrique. Ensayos de informática jurídica. México: Fontamara, 1996, p. 18.

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 *e-commerce*, 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.

Si bien para la época en que sucedieron los hechos (22 y 23 de noviembre de 2007) no 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»*[14], si 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»*, el cual ha sido aprobado o adoptado por el organismo nacional de normalización (art. 2, literal b), es decir por ICONTEC (Instituto Colombiano de Normas Técnicas y Certificación).

Dicha norma técnica es la NTC NTC-ISO/IEC 27001 sobre *«Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI)»* y los requisitos de estos, la cual corresponde a una adopción idéntica por traducción de su documento de referencia que es la norma ISO/IEC 27001[15], que es un estándar

---

14 El órgano de vigilancia estableció que la implementación de la circular tendría lugar en tres etapas; la primera inició el 1° de julio de 2008 y la última finalizó el 1° de enero de 2010.

15 ISO corresponde a las siglas en inglés de International Organization for Standardization e IEC a la International Electrotechnical Commission. La primera tiene como misión la creación de estándares internacionales en diferentes áreas y la

internacional para la «*seguridad de la información*» aprobado y publicado en octubre de 2005, reconocida como la principal pauta técnica a nivel mundial en esa materia, de ahí que muchas entidades públicas y privadas busquen certificarse en ella, es decir, que una entidad de certificación externa, independiente y acreditada audite su sistema y determine si se encuentra conforme a dicho estándar.

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*

---

segunda es la principal organización en el mundo que elabora estándares internacionales para las tecnologías eléctricas, electrónicas y relacionadas.

confidencialidad, integridad y disponibilidad puede tener sobre estos activos» para después *«e) 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 a partir de los criterios establecidos en el numeral 4.2.1, literal c)»* 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.».*

4.3. 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»*[16], e imponen, de modo

16 SIMÓN HOCSMAN, Heriberto. Negocios en internet. E-commerce, correo electrónico, firma digital. Buenos Aires: Edit. Astrea, 2005, p. 238.

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»*.[17]

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 el *e-commerce*, siendo 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»*.[18]

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*

17 Numeral 3.13 de la NTC-ISO/IEC 27001, tomado de la NTC-ISO/IEC 17799:2006.
18 Anexo A NTC-ISO/IEC-27001 (A.10.9, A.10.9.1 a A.10.9.2).

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.[19]

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, siendo requerida la

19 Anexo A (A.11.4.4, de A.11.4.5 a A.11.4.7; A.11.5 de A.11.5.1 a A.11.5.6.

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, rodeando 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.

4.4. Las modalidades de fraude electrónico:

Entre las 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, incorporando mecanismos detectores en cajeros electrónicos y datafonos.

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.

Scam: Los tipos más frecuentes son el phishing, el

hoax y el pharming, pero de ellas la primera y la tercera son las más empleadas para la disposición o retiro ilícito de los dineros depositados en cuentas bancarias.

Phishing: El término procede de la palabra «*fishing*» que quiere decir pesca, y es una forma de fraude electrónico «*caracterizada por intentos de adquirir datos personales de diversos tipos: contraseñas, datos financieros como el número de las tarjetas de crédito y otros datos personales*».20 Su creación «*data de mediados de 1996, cuando los crackers que practicaban el robo de cuentas de la América Online (AOL), defraudaban contraseñas de usuarios*».21

En sus versiones primarias se caracteriza por engañar a los usuarios para conseguir datos que son confidenciales, tales como las claves de acceso a la cuenta bancaria en la página web del Banco; el estafador envía mensajes a miles o tal vez millones de direcciones de correo electrónico previamente recolectadas en internet aprovechando los servidores de e-mail mal configurados; en los mensajes que tienen la apariencia de provenir de sitios web de entidades financieras, notifican la necesidad de confirmar la información relacionada con la cuenta por razones diversas como modificaciones del protocolo de seguridad; la cancelación del producto por no actualizar los datos; personalización del acceso para el cliente, entre otros.

El mensaje viene con el logotipo de la entidad bancaria, su publicidad usual y demás signos distintivos como gráficos, imágenes e incluso el código del establecimiento bancario, para generar confusión en el

20 ARIAS, Ángel. Las estafas digitales. It Campus Academy, 2014.
21 Ibídem.

cliente y a través de un link o vínculo hace enrutamiento a un sitio web que aparentemente es el de la entidad, pero en realidad en un sitio falso o «*sitio spoof*», en el cual al ingresar el cliente su información de autenticación (usuario y clave), el cibercriminal la recibe y posteriormente usa en transacciones como transferencia a cuentas, compras o pagos.

Esa modalidad delictiva también se puede realizar de otras maneras más difíciles de detectar por el cliente, siendo las más comunes el ataque al servidor DNS, las URL falsas, los formularios HTML falsos en correos electrónicos, vishing y por mensajería instantánea.[22]

La primera[23], consiste en corromper el DNS o sistema de nombres de dominio en una red de ordenadores (envenenamiento de la caché del DNS), llevando a que la URL que es el localizador de recursos o de direcciones www de una web apunte hacia un servidor diferente del original, de modo que al digitar o introducir la dirección correcta de la página web a la que se desea acceder, si el DNS ha sido corrompido, apuntará a una página falsa hospedada en otro servidor con otra dirección IP que tendrá la apariencia de la del Banco, en la que el cliente ingresa sus datos, los cuales son capturados; la transacción que intenta el cliente arroja error porque no es la página real y el ciberdelincuente logra su cometido de capturar o «*pescar*» la información, modalidad que ahora es conocida como «*pharming*». Muchas

---

22 Ibídem.

23 Esta modalidad habría sido la empleada en el caso de Tax Individual S.A. según el concepto rendido por el experto consultor informático citado por la empresa (fl. 83, c. 1).

veces no es posible ver toda la extensión de la dirección de la página (URL) por la limitación de espacio de algunos computadores portátiles y de dispositivos como los smartphones.

En la segunda forma, se crean URL extensas que al usuario se le dificulta identificar y que simulan la dirección real que aparece en el campo de la parte superior del navegador de Internet, y el candado que aparece en la esquina inferior derecha, por lo que al mirar el inicio de la dirección www cree estar en la zona transaccional segura de la entidad financiera, pero la verdad es que ha ingresado al sitio web de un dominio controlado por el defraudador.

Los formularios HTML falsos remitidos por e-mail conducen al usuario a dejar a disposición del delincuente la información que supuestamente requerida por el Banco, en verdad fue solicitada por el defraudador, el cual con esos datos no necesita simular o clonar la interfaz de la entidad para engañar a sus clientes.

En el vishing, el defraudador acude a mensajes de texto (SMS), e-mails o correos de voz para propagar comunicaciones supuestamente provenientes de la entidad financiera que solicitan datos confidenciales o piden redireccionarlas a otro número y hablar con alguno de los defraudadores.

La comunicación informal que se establece a través de la mensajería instantánea es aprovechada por los delincuentes para hacerse pasar por amigos o familiares de

la víctima, pero al abrir el mensaje se instala en el ordenador un malware (programa o código malicioso) a través de los cuales puede implantarse un *keylogger* o registrador de las pulsaciones realizadas en el teclado del computador, las cuales archiva en un fichero y envía a través de internet, permitiendo el acceso de terceros a contraseñas e información privada.

La exposición de las modalidades reseñadas de fraude revelan no solo que las contraseñas y palabras clave (PIN) ya no son mecanismos suficientemente confiables y seguros, porque pueden ser interceptados durante la transmisión de los datos vía internet y tienen, por tanto, un alto grado de vulnerabilidad, lo que obliga a adoptar herramientas más seguras y dinámicas, porque es la plataforma tecnológica la que debe proveer los medios técnicos de seguridad que se requieran para que solo los titulares de los productos sean los que dispongan de sus dineros, minimizando la vulnerabilidad del sistema informático. Los métodos de defraudación son cada vez más sofisticados, de manera que al cliente le es prácticamente imposible detectarlos antes de la sustracción de dinero de su cuenta.

5. 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, siendo 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 atendiendo 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*».

6. Hechas las anteriores precisiones, debe la Sala ocuparse de las acusaciones planteadas en el único cargo que formuló el casacionista.

6.1. Cuestionó el censor la interpretación dada por el *ad quem* a la demanda, en relación con lo cual es necesario reparar en que dicho sentenciador circunscribió el problema jurídico a resolver en la determinación de «*si corresponde endilgarle responsabilidad a la entidad bancaria por el fraude a la cuenta de ahorros de uno de sus clientes, hecha a través del portal de internet, atendiendo la específica y profesional función de cuidado y custodia de dinero*», lo que está acorde con las pretensiones de la demanda.

A su vez, al delimitar el marco normativo y jurisprudencial, fuera de los artículos 1494 y 1495 del Código Civil, indicó que «*en el evento en que el contrato recae sobre el depósito de dinero en una entidad bancaria, esta actividad está regulada en el Código de Comercio en el Título XVII "De los Contratos Bancarios", refiriéndose lo relativo a la cuenta corriente, depósito a término y depósito de ahorro*», dentro del cual queda comprendido precisamente el artículo 1398 que da pie a la reclamación.

Lo que complementó con resaltar del precedente jurisprudencial que «*el artículo 733 del Código de Comercio, en*

tanto contempla un supuesto particular, se sustrae del principio general de responsabilidad a cargo de la entidad bancaria por el riesgo profesional que se deriva del ejercicio y del beneficio que reporta su actividad financiera especializada», que era la razón de ser de invocarlo.

Esto es, se quiso resaltar el «***principio general de responsabilidad bancaria***», para enfatizar en que «*[i]rrumpe de la jurisprudencia de la Corte Suprema de Justicia, en relación con la responsabilidad bancaria, que se ha adoptado el reclamo de deberes especiales de diligencia al sistema financiero, por la confianza pública depositada en las instituciones bancarias, para derivar su responsabilidad civil del ejercicio y del beneficio que reporta su especializada actividad financiera*».

Mucho menos fue desacertada su alusión a que el «*artículo 98 numeral 4 del Dec. 663 de 1993 (...), obliga a sus instituciones financieras a "emplear la debida diligencia en la prestación de los servicios a sus clientes" lo mismo que a sus administradores el de "obrar no sólo dentro del marco de la ley sino dentro del principio de la buena fe y de servicio a los intereses sociales" (artículo 72)*», pues, a pesar de que están en su redacción original y se les introdujeron cambios antes de la ocurrencia de los hechos, no variaron en su esencia y alcances.

Por un lado, el artículo 72 del Estatuto Orgánico del Sistema Financiero, en su primer inciso, se refería a las «*reglas de conducta de los administradores*» pero la modificación del 12 de la Ley 795 de 2003, las extendió a las «*entidades vigiladas (...) directores, representantes legales, revisores fiscales y funcionarios*», quienes «*deben obrar no sólo dentro del marco de la ley sino dentro del principio de la buena fe y de servicio al interés público*

de conformidad con el artículo 335 de la Constitución Política», siendo relevante que pasó de hablarse de los «*intereses sociales*» al «*interés público de conformidad con el artículo 335 de la Constitución Política*».

En cuanto al artículo 98 numeral 4, si bien fue afectado con el artículo 24 de la Ley 795 de 2003, se conservó el que las «*instituciones sometidas al control de la Superintendencia Bancaria, en cuanto desarrollan actividades de interés público, deberán emplear la debida diligencia en la prestación de los servicios a sus clientes*», lo que mantuvo vigencia hasta el 30 de junio de 2010, cuando ya estaba trabada la litis.

Como el sentido de las normas no se alteró, quiere decir que las conclusiones del sentenciador de que la «*debida diligencia*» exigida era «*la de un profesional que deriva provecho económico de un servicio en el que existe un interés público*» y que la responsabilidad por no cumplirla en forma solo se resquebraja «*si por culpa del cuenta habiente o de sus dependientes o representantes, se produce un pago o se materializa un traslado u otro tipo de operación en el que se comprometan recursos del cliente con base en fraudes*», no comporta desconocimiento alguno del régimen de responsabilidad aplicable, según se destacó líneas atrás.

6.2. Limitando los cuestionamientos a la valoración de los medios de convicción, de donde dedujo el fallador la «*orfandad probatoria*» tanto de las seguridades tomadas por el opositor para impedir la ocurrencia de los riesgos derivados de transferencias electrónicas, como de la falta de cuidado y diligencia del cliente en el manejo de la clave, tampoco encuentra prosperidad la acusación por estas

razones:

a). Si bien se resaltan las deficiencias demostrativas en esos dos aspectos puntuales, el primero de ellos resulta irrelevante frente a los planteamientos que demarcaron el alcance de la responsabilidad civil bancaria, ya que se entendió derivada del «*ejercicio y del beneficio que reporta su especializada actividad financiera*» y sin piso únicamente de existir «*culpa del cuenta habiente o de sus dependientes o representantes*».

Quiere decir 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.

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.

En otras palabras, 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 la visión que expone el recurrente de las probanzas que dice desatendidas no logra desvirtuar la deducción del Tribunal sobre la falta de asidero a las «*afirmaciones del Banco en relación con las seguridades que dice haber tomado para impedir la ocurrencia de los riesgos propios de la actividad realizada por medios electrónicos o Internet*», siendo que lo sucedido lejos de ser un caso aislado o único, obedecía a un patrón ya detectado por la entidad financiera y que, independientemente de su magnitud, ameritaba de medidas urgentes correctivas y preventivas para evitar su ocurrencia.

Aunque se recalca la relevancia de lo testificado por Carlos Alberto Botero Vélez sobre el cumplimiento de normas técnicas internacionales relacionadas con la seguridad de la información y gestión de riesgo, así como las circulares de los organismos de vigilancia, se omite que al preguntársele sobre su conocimiento de «*casos similares a los que hoy nos ocupa en este proceso de fraude electrónico de sus clientes*» respondió que «*si tengo conocimiento de otros casos, a nivel de Banco AV Villas se registran aproximadamente cinco reclamaciones año, esto para personas jurídicas, lo cual no es frecuente, y representa un porcentaje insignificante frente al nivel transaccional*», añadiendo que «*los volúmenes de reclamación en pesos oscilan entre cien y doscientos cincuenta millones de pesos. Esos cinco casos que se reportan son similares a los reclamados por el cliente Tax Individual*» (fl. 10 cno. 3).

A su vez, José Isaías Gracia Rodríguez encajó la

situación dentro de la «*modalidad delictiva denominada Phissing*», conocida «*hace unos cinco años para acá a nivel mundial*», esto es, aproximadamente desde 2004 ya que declaró el 9 de septiembre de 2009, concordando con el otro deponente en que ocurrieron hechos similares en la entidad demandada. Y si bien expuso que «*se ha demostrado, como en este caso, que se trató de páginas falsas enviadas por delincuentes y en los que los empleados autorizados de las empresas contestaron los correos falsos y de esa manera los delincuentes obtuvieron claves que permitieron transferir datos*», tal seguridad se contradice cuando relató en un comienzo que «*al parecer personas desconocidas enviaron una página falsa del Banco Comercial AV Villas S.A., la cual fue respondida por los usuarios y personas que tenían los permisos de Tax Individual para accesar al medio de Internet del Banco Comercial AV Villas S.A.*».

Más allá de que los dos declarantes insistieran en la toma de seguridades por el contradictor cumpliendo estándares nacionales e internacionales, lo cierto es que a pesar de ser múltiples los casos semejantes al de la promotora en donde se daban pérdidas considerables para los clientes, así no lo fueran para AV Villas, ni siquiera existe certeza de cómo se fraguó la defraudación, lo que respalda la apreciación del Tribunal de que sus manifestaciones «*en nada permiten afirmar que la entidad bancaria haya cumplido con la obligación que se le exige, por la actividad profesional y especializada que ejerce, de brindar mayor seguridad en el uso de los servicios que ofrece en especial cuando de medios electrónicos se trata*».

Ni siquiera se revalúa eso con la certificación del Gerente de Contabilidad de AV Villas donde consta el pago de $71'372.245 a la firma Etek International Holding Corp.,

ni con las impresiones donde constan todos los datos de las operaciones en los diferentes canales, incluido internet, puesto que la discusión no era la ausencia de medidas de seguridad o la falta de registros individualizados sino que eso no fuera suficiente.

Tampoco se desvirtúa con la ausencia de restricciones informadas por la gestora, diferentes al monto de las operaciones diarias, puesto que la inexistencia de las mismas no disminuye el grado de responsabilidad del Establecimiento Bancario. Si bien el cliente tiene 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, debiendo asumir las pérdidas si el comportamiento del titular o sus autorizados estuvo acorde con las directrices impartidas.

Y no puede decirse que la manifestación en el hecho séptimo de la demanda de que «*la consulta a través del portal de Internet del Banco durante más de cinco (5) años de operación no presentó nunca ninguna anomalía, ni mucho menos los miles de operaciones de recaudo y las transferencias electrónicas que constantemente realizaba el señor Johan Mosquera*» constituya confesión «*del alto grado de diligencia y seguridad del Banco en el manejo de su servicio a través del portal de internet*», como lo plantea el impugnante, como si eso fuera perjudicial a sus intereses. A lo sumo escenifica es el alto grado de confiabilidad que le daba esa forma de manejar recursos, pero se fracturó el 22 y 23 de noviembre de 2007 cuando pasó todo.

Los elementos de convicción que se denuncian como mal apreciados, ya sea individualmente o en conjunto, no logran desvirtuar la conclusión del sentenciador 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.

b). En lo que respecta a la observación del *ad quem* de 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 cargo evidenciar el desfase endilgado.

La argumentación del ataque se centra en que los empleados de la accionante pese a recibir «*un aviso de AV Villas indicando que el acceso estaba bloqueado por 12 horas, y a pesar de manejar a través de la misma una cuenta de recaudo, no se tome ninguna acción ni proceder, sino que se guarde total silencio y omisión*», sin embargo estos mismos relataron que no era algo extraño porque ya había ocurrido con antelación sin repercusiones.

Siendo usual que para facilitar el acceso de los usuarios y corregir problemas de programación las páginas web y portales de internet se sometan a mejoras en el diseño, el mero llamado de atención de que el «*servicio se restablecerá en aproximadamente 12 horas*» no era suficiente

Además, en un aparte que omite el recurrente, fue enfático Yeison Ferney en que el mensaje de suspensión por 12 horas «*no se consideró irregular ya que en ocasiones anteriores al funcionario del área de contabilidad le había sucedido que la página no estuviese disponible para acceso y que la misma le solicitara un ingreso posterior*» y más adelante expuso que la «*página web con la cual se comete el engaño o phising es completamente idéntica a la página suministrada por el banco, por lo cual no es posible para un usuario normal identificar dicho engaño...*» (fl. 283 cno. 2)

De tal manera que frente a una advertencia usual y rutinaria, cuya fraudulencia no era detectable a simple vista, luce razonable que la empleada se limitara a cerrar la página de internet sin pedir corroboración de su compañero de trabajo Johan Mosquera Lozano o la persona encargada de prestar soporte en sistemas, el que era ajeno a las procedimientos internos del Banco.

La denuncia formulada por Sonia Quintero, en nada se opone a esa justificación, y si allí se toca que se recibió un «*correo de Colmena que decía que la dirección IP de nosotros estaba siendo utilizada por usuarios no reconocidos del Banco y nosotros llamamos al banco a verificar si ese correo era de ellos y nos dijeron que no*», es porque se refiere al día siguiente al del reporte de inconvenientes técnicos, lo que ahí si despertó sospechas y provocó la reacción inmediata para constatar lo que estaba pasando con las cuentas de la gestora.

Es más, la diferencia no tan ostensible en la dirección electrónica «*http://www.avvillas.com.co/transac-bbs*», en la que falta la «*s*» en el «*hipertexto "http"*», como lo entendió el Tribunal, quedó explicada por Javier Andrés Arango Salazar y en extenso se transcribe por su relevancia

> *PREGUNTA: ¿Díganos, si la página del Banco Comercial AV. Villas S.A. que fue suplantada y que Ud. conoció es la misma que aparece en el expediente en el cuaderno principal a folio 24 el cual se le pone de presente? RESPUESTA: Sí. Esto es la página falsa con la cual se hizo la suplantación de identidad del Banco Comercial AV. Villas S.A. Este es el mensaje que le apareció al usuario cuando trataba de ingresar supuestamente a la página de Banco Comercial AV. Villas S.A. - Yo afirmo que es la página falsa porque esta no posee un certificado digital, es más, la URL es diferente ya que no es HTTPS sino HTTP, pues si la página cuenta con un certificado digital siempre será HTTPS, y eso se puede observar en la URL (en la parte superior en azul), http es el protocolo universal para navegar en Internet y el https es el mismo protocolo modificado de manera segura y se utiliza cuando se va a transmitir información confidencial ya que cifra los datos. La utilización de estos protocolos depende del dueño de la página, en este caso Banco Comercial AV. Villas S.A. PREGUNTA: ¿Díganos si el Banco Comercial AV. Villas S.A. pudo haber tomado medidas para evitar que el funcionario de Tax Individual S.A. al intentar ingresar a su página no fuera desviado a un protocolo no seguro como aconteció en este caso? RESPUESTA: Sí, a través de medidas de seguridad como una VPN. - PREGUNTA: ¿Díganos si es lo mismo un mensaje de Internet o de correo y una página de Internet? RESPUESTA: Normalmente los mensajes de Internet se transmiten a través de correos o de conversaciones tipo chat. En el caso de fraudes de este tipo de delitos informáticos con los bancos, lo que normalmente se utilizan son mensajes a través de correos que*

incitan a que el usuario de clik (sic) *sobre el mensaje de manera que abra una página de Internet. -Una página de Internet es un portal donde se carga información o se pueden hacer operaciones como en el caso de los portales de los bancos. El folio 24 del expediente es una página de Internet. -PREGUNTA: ¿Díganos si el fraude mediante Phishing que ocurrió en nuestro caso se presentó a través de una página falsa o por medio de un mensaje de correo? RESPUESTA: Se presentó a través de una página falsa y como mencioné anteriormente no encontré un mensaje de correo de este tipo. PREGUNTA: ¿Teniendo en cuenta su conocimiento sobre la materia, díganos si es posible que un usuario al digitar correctamente el nombre de una página de Internet sea redireccionado hacia una página falsa? RESPUESTA: Sí, completamente, por cualquiera de los métodos que explique antes, que son o modificando los registros DNS de un computador (archivo host) o haciendo un envenamiento a uno de los servidores DNS. PREGUNTA: ¿Teniendo en cuenta sus conocimientos sobre la materia, díganos que tan fácil es detectar un fraude mediante Phishing a través de página, por parte de un usuario normal? RESPUESTA: Si no ha sido instruido en la materia es difícil, por ejemplo lo que le estaba mostrando en esta página de folios 24, porque la página falsa es exactamente igual a la original y si uno no sabe cosas como lo del certificado digital para lo cual necesita haber sido instruido, no va a notar la diferencia. Tal diferencia en este caso se puede evidenciar en la URL donde debe estar https en vez http y el navegador de Internet, por ejemplo el Internet Explorer carga un candado amarillo.*

La claridad de esa narración que provino de un «*oficial de seguridad informática del Municipio de Medellín*» y se enteró de lo sucedido al poco tiempo por contactarlo la demandante, con quien tuvo nexos de consultoría sin que por ello se observe amañada o con el ánimo de favorecerla,

resiste cualquier confrontación con las versiones de Carlos Alberto Botero Vélez y José Isaías Gracia Rodríguez quienes frente a similares inquietudes fueron vacilantes en identificar a qué obedecieron los movimientos discutidos.

Por lo tanto, el esbozo dibujado por el censor obedece a una interpretación particular de los documentos y declaraciones que señala como indebidamente tasados, pero sin estructurar una cohesión que demuestre la equivocación que endilga al Tribunal, dejando incólume la razón puntual que dio lugar a la confirmación del fallo condenatorio de primer grado.

Fracasa, por lo expuesto, el cargo.

Las costas del recurso extraordinario se impondrán al impugnante, y para la tasación de las agencias en derecho, se tomará en cuenta que la demandante presentó oposición.

III. DECISIÓN

En mérito de lo expuesto, la Sala de Casación Civil de la Corte Suprema de Justicia, administrando justicia en nombre de la República y por autoridad de la ley, **NO CASA** la sentencia de treinta de julio de dos mil trece, proferida por la Sala Séptima de Decisión Civil del Tribunal Superior del Distrito Judicial de Medellín en el proceso ordinario antes referenciado.

Costas a cargo del Banco Comercial AV Villas S.A. y a favor de Tax Individual S.A. Inclúyase la suma de

$6'000.000 por concepto de agencias en derecho.

En su oportunidad, devuélvase el expediente a la Corporación de origen.

NOTIFÍQUESE

ÁLVARO FERNANDO GARCÍA RESTREPO
Presidente de Sala

AUSENCIA JUSTIFICADA
MARGARITA CABELLO BLANCO

AROLDO WILSON QUIROZ MONSALVO

LUIS ALONSO RICO PUERTA

ARIEL SALAZAR RAMÍREZ

LUIS ARMANDO TOLOSA VILLABONA