

**República de Colombia
Rama Judicial**



**TRIBUNAL SUPERIOR DE BOGOTÁ, D.C.
SALA CIVIL DE DECISIÓN**

Bogotá, D.C., ocho (08) de septiembre de dos mil veinte (2020)

11001 31 99 003 2019 03463 01

Por encontrarse legalmente procedente, el Despacho dispone:

Admitir en el efecto **SUSPENSIVO** el recurso de apelación interpuesto por la parte demandante, en contra de la sentencia emitida el 13 de julio de 2.020, por la Delegatura para Funciones Jurisdiccionales de la Superintendencia Financiera de Colombia, dentro del asunto de la referencia.

Para los fines a que haya lugar, póngase en conocimiento de la parte demandada el escrito mediante el cual el extremo activante manifestó sus reparos contra la decisión de primer grado.

Por Secretaría, una vez cobre ejecutoria la presente decisión, contrólense los términos con los que cuentan las partes para sustentar la alzada interpuesta, conforme lo consagra el artículo 14 del Decreto 806 de 2.020.

NOTIFÍQUESE,

A handwritten signature in black ink, appearing to read 'Juan Pablo Suárez Orozco', written in a cursive style.

**JUAN PABLO SUÁREZ OROZCO
Magistrado.**

Señores:

SUPERINTENDENCIA FINANCIERA DE COLOMBIA
DELEGATURA PARA FUNCIONES JURISDICCIONALES
L.C.

Número de Radicación : 2019151999-037-000
PROCESO VERBAL Expediente : 2019-3463
Demandante : MUNICIPIO DE RONCESVALLES - TOLIMA
Demandados : BANAGRARIO

ALVARO ANDRES BUITRAGO CADAVID, mayor de edad, domiciliado en Ibagué (Tolima), identificado con C.C. 94.410.951, portador de la T.P. 109.439 del C.S.J., en mi calidad de apoderado judicial de la demandante acudo dentro de los términos otorgados, a su despacho para sustentar el recurso de apelación impetrado contra la decisión de fallo proferido dentro del presente proceso, lo cual hago en los siguientes términos

PETICION

Solicito a los honorables magistrados que se acceda a las pretensiones de esta apelación y se modifique la decisión del fallo proferido por la superintendencia financiera de Colombia el 13 de julio del presente año, dentro del proceso de la radicación de la referencia, y en su lugar se ordene al banco agrario de Colombia como consecuencia de la declaratoria de responsabilidad a la devolución de los recursos que fueron defraudados de las cuentas de ahorros del municipio de Roncesvalles Tolima y que se encuentran determinadas en el escrito petitorio del presente proceso.

SUSTENTACION DEL RECURSO

Sustento el recurso, y determiné los reparos contra el fallo proferido en primer instancia en que el mismo se sustentó en que la demandada había obrado de acuerdo a lo conceptuado en el contrato, sin entrar a determinar de manera directa frente al material probatorio, la forma en que la misma había actuado transacción por transacción, en especial determinando de manera concreta y certera cuáles habían sido los procedimientos que dieron al final como resultado la defraudación de las arcas del municipio de Roncesvalles.

La carga de la prueba sobre la responsabilidad del mal manejo de la cuenta, caía en la demandada quien debía haber aportado siquiera de manera enunciativa y haber

demostrado de manera documental como había sido el proceso de envío de los token así como la utilización de las claves determinadas por mi representada, Y no simplemente señalarse que sea cogía a que el banco había realizado las operaciones basado en las claves que había entregado, lo cual no quedó demostrado en el proceso, pues no hay documento o prueba que determine que hay igualdad de características entre los canales registrados por el municipio y los canales de comunicación utilizados para enviar las claves y las autorizaciones. Igualmente que las claves enviadas fueron las mismas utilizadas para acceder al sistema, Y que las autorizaciones de dicho sistema fueron realizadas con claves enviadas por el banco al respectivo usuario registrado como autorizador.

Determinar el juzgador de primera instancia que el municipio no fue diligente en la custodia de las claves que a él le fueron entregadas y por ende su incumplimiento contractual, debía tener sustento en pruebas que efectivamente hubieran demostrado siquiera que las claves utilizados eran las mismas que estaban bajo la custodia del municipio y no otras.

Pues si las claves utilizadas fueron las entregadas al municipio no cabría ninguna duda de la responsabilidad de este sobre las mismas. Pero si las claves utilizadas fueron otras era el banco a quien le tocaba responder por la pérdida de esos recursos.

Como no se allegó prueba que el banco al momento de habilitar las transacciones utilizó las mismas claves enviadas mal podría como hizo el juzgador, afirmar que quien falló en la custodia de esas claves había sido el municipio.

Las medidas de precaución de la entidad financiera pueden sobre los contratos establecer estándares de seguridad necesarios para que no fuesen vulnerados por terceros. Frente al perfil de las costumbres transaccionales del cliente el banco debía proceder a revisar si las operaciones efectuadas eran normales en el cliente en este caso mi representado. Sin embargo no sólo porque las mismas eran frecuentes, si no porque los montos que se iban de evitando eran similares en su cuantía que no superaban los 2,400,000 pesos ni descendían de 2,100,000 pesos en su mayoría con una continuidad de minutos entre una y otra, así como a beneficiarios sobre los que anteriormente no se había realizado ningún tipo de giro, pero más aún sospechoso es que todos eran provenientes de un solo banco que para el caso era Bancolombia. Igualmente se resalta la operación de una cuenta a nombre Luz Marina Prada cuentahabiente Bancolombia número 1-540-002-7860 la cual durante los días 8 de marzo, 11 de marzo, 12 y 13 de marzo, retiro en seis ocasiones más de 35 millones de pesos en cada una de ellas llegándose incluso a hacer traslados de hasta tres veces en un día por esas sumas.

No era factible que al banco y no le llamara la atención esta situación y por el contrario el mismo debía haber establecido todos los protocolos de seguridad ante el giro constante que se realizaba a una misma cuenta de valores tan altos, Como si no pudiese ser realizado

en uno solo por un valor más alto.

Ha establecido la jurisprudencia de la corte suprema de justicia sala de casación civil, en espacial mediante radicación Radicación n° 05001-31-03-001-2008-00312-01, que “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 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.

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).”

Igualmente ha dicho esa corte frente a 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.”

“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.”

“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».

En ese orden de ideas correspondía al banco Banagrario demostrar de manera fehaciente que la defraudación de que fue víctima mi cliente se debía por responsabilidad de este y no simplemente enunciando cuál es eran los métodos de control que utilizaba el banco.

Sobre el particular jamás se demostró en este proceso que el banco hubiese realizado los envíos de las claves de token a los números que para tal efecto había determinado mi cliente en el documento referido.

Si el documento al tener en cuenta corresponde al presuntamente remitido por el señor alcalde municipal de la época y radicado al banco el 28 de febrero de 2018 los números de

teléfono y correos de quienes realizaban la labor de auditor y usuario administrador eran diferentes a los números de teléfono donde presuntamente se enviaron los mensajes.

Nótese que en ese oficio se establece de manera clara como nombre del usuario **auditor** de la empresa al señor Norberto Rodríguez Sánchez identificado con la cédula de ciudadanía número 5.989.003 Y de la misma forma establece que el citado señor Norberto Rodríguez Sánchez fungiría como **administrador** del portal.

No obstante ser anunciada esta prueba y ser fundamento además del fallo proferido en primer instancia desconoce esta parte porque no se tuvo en cuenta que en la misma se relacionaban los números de teléfono y correos electrónicos en los cuales contestaría y se generarían las alertas seguramente para el manejo de las cuentas del municipio de Roncesvalles.

Es así como el número de teléfono consignado en dicha prueba que aporta incluso la parte demandada corresponde al 312-457-8921 y el correo electrónico corresponde a hacienda@roncesvalles-tolima.gov.co.

Anterior Van agrario dentro del proceso jamás demostró según se considera de los soportes presentados al mismo que había remitido tanto a ese teléfono como a ese correo electrónico la información correspondiente a los movimientos que se estaban realizando de la respectivas cuentas y que a la postre determinaría la defraudación a mi representada. Los sistemas de seguridad eran claros en advertir una serie de pasos para poder confirmar que no se estaba suscitando en algún momento del uso de la banca virtual un proceso de saqueo de las cuentas como ocurrió en los días materia del proceso.

Desde un principio el municipio de Roncesvalles ha sido claro en determinar que no recibió los token y que no fue él quien aplicó dichos token o claves en las respectivas transacciones que así lo solicitaban.

Llama a la atención igualmente que determina el señor testigo de la parte demandada Felipe González Adams de asegurar la operación funcional de lo que se llaman canales virtuales en especial la banca virtual que es la que atañe a este proceso.

Sobre el particular manifestó en su declaración que se encuentra en el audio de la audiencia minuto (01:38:20) que para el proceso de radicación de modificaciones de el usuario administrador en la banca virtual se requerían cinco documentos, el usuario administrador del quiérente es el que se va encargar de hacer toda la administración del portal, procedimiento para vinculación es estricto y está realizado de la siguiente manera con cinco documentos que se deben radicar de manera física en las oficinas del banco mediante los cuales el representante legal del cliente le informa al banco quién es el que va a hacer

responsable del portal, un formato de novedad del cambio de administración y donde se administra el contacto del administrador, una copia del acta de posesión de la persona que está autorizando en este caso el alcalde municipal, copia de la cédula del usuario administrador y unos formatos de actualización de productos del banco.

Una vez verificado eso se hace un pre registro realizado por el usuario administrador donde fija su nombre de usuario su número celular su correo electrónico y asignar una clave personal para el usuario que está cifrada Y registra principalmente quién va a ser el usuario auditor y ese usuario es quien va a tener conocimiento de todas las acciones que va a tener el administrador.

Este usuario auditor es el que va a tener el control sobre todo lo que realice el administrador en el portal sin que pueda tener un usuario al ingreso de la banca virtual pero se lo notifican las acciones del usuario administrador.

El banco tenía que hacer una revisión de conformidad de la información y que corresponda al pre registro realizado por el usuario administrador, si el correo electrónico es diferente al rechazado en el registro se debía a rechazar según determinó el testigo.

Debían hacer una revisión de firmas y que esas firmas correspondía al representante legal y de esa forma si se autorizaba la modificación en el sistema.

Posteriormente se genera un token de 12 minutos al teléfono o si no el mismo vence y en este caso como es una persona jurídica oficial tienen un servicio de autenticación fuerte de manera obligatoria.

Se hace un registro de seguridad de la máquina y el sistema lo que hace es que captura la información de la máquina y genera una huella de seguridad y cada vez que el usuario tendría que entrar a la banca virtual esa huella que tomo ese computador será verificada o validada por el banco en ese momento corroborando que la huella corresponda con la registrada.

Si bien es cierto se manifiesta por parte de la demandada así como se acoge por parte del fallado que las operaciones reclamadas por el municipio fueron realizadas con la información transaccional que debía encontrarse en custodia exclusiva en ninguna parte del proceso aparece que fue dicha información la que se ingreso para realizar los movimientos.

De haber sido así era deber del banco demostrar que las claves y accesos a los cuales se procedió a utilizar por parte de quién había extraído el recurso habían sido generados con las claves o las medidas de seguridad que habían sido entregados por parte del

administrador al banco.

Fue dirigente el mismo en demostrar que las operaciones desconocidas del municipio fueron notificadas al número telefónico 310-887-1008 y para tal demostración remitió un listado de notificaciones SMS las cuales si se lee dentro del material probatorio no informan a quien se le realizó para que de esa forma una entidad pública pudiera sugerir si la misma se trataba de un fraude o de una transferencia legalmente realizada.

Por eso no basta simplemente con la firmar que se había informado mediante el mensaje SMS la realización de una transferencia virtual ordinaria además en el ejercicio de la operación financiera de las entidades públicas, si no que debía haberse demostrado dentro del proceso que dicha transferencia se había realizado mediante los canales válidos y oficiales utilizando las claves de seguridad o token que se habían emitido hacia los números celulares de quienes actuaban como originador o autorizador Y que las mismas habían sido realizadas a cuentas previamente inscritas por ellos para efectos de realizar los traslados.

Simplemente sugerir en el proceso que las operaciones se habían realizado con las claves asignadas y los códigos de seguridad token enviados no podía ser suficiente para demostrar que esto fue así, dicha información sólo estaba en poder de la demandada y era ella a quien le correspondía entrar a demostrar que las claves con las que se violó el sistema eran las que habían sido entregadas al usuario lo cual desde un principio esta parte ha afirmado que no es cierto y que no existe ninguna clave remitida a los números celulares O correos electrónicos asignados que hubiese sido generados por la demandada.

Tomar esta situación por el contrario invertiría la carga de la prueba y pondría en este caso a la administración municipal de Roncesvalles a demostrar cuáles fueron las claves utilizadas y si las mismas corresponden a las que le pertenecían o que le habían sido asignadas, información que por simple lógica no posee pues la misma reposa únicamente en los archivos físicos o digitales del banco y de su seguridad y no en poder de la administración municipal aquí demandante.

Trasladar la carga de la prueba de que la defraudación no ocurrió por culpa del cliente del banco desproporcional en la medida en que quien debe demostrar cuáles fueron dichas claves a qué horas fueron enviadas las mismas y a qué correo fueron enviadas le correspondía era al banco quién era el emisor de estas.

Bajo el anterior cualquier proceso ante esta jurisdicción por pérdida de recursos de las cuentas bancarias será fallada a favor de los bancos pues ellos simplemente se encargan de afirmar que enviaron las claves a los números correspondientes y que los sistemas de seguridad y verificación utilizados fueron los entregados para que se exoneren de responsabilidad sin demostrar absolutamente nada.

Debe recalcar esta parte que no era una prueba ni siquiera humana sino documental, pues copia de los correos con las claves de habilitación así como copia de los mensajes de información al auditor de la cuenta por modificaciones que hiciera el administrador, E igualmente los registros de creación y aprobación de los traslados sólo están en poder del banco y era quien debía aportarlos a este proceso para demostrar que habían sido correctamente enviados y utilizados, Y no simplemente aduciendo que enviaron una notificación de traslado sin determinar siquiera a qué cuenta se hacía la misma y cuál era su beneficiario.

Sin embargo de la misma forma que enviaron un mensaje de notificación que ya había ocurrido un traslado entre cuentas se debió haber aportado este proceso la prueba de que dicho traslado se había realizado mediante los canales y medidas de seguridad establecidas por el banco, la única forma entonces en que los recursos se hubieran extraviado era porque esa información y esas medidas habían sido entregadas a terceros por parte de los funcionarios del municipio lo cual nunca se demostró.

Es lógico que si fueron los mismos funcionarios del municipio los que instauraron la denuncia, qué son los mismos funcionarios del municipio los que iniciaron esta reclamación, es porque tienes la certeza que no fueron ellos quienes de manera fraudulenta manejaron los sistemas del banco.

La única prueba que hay de cómo se realizaron los movimientos y en qué forma se entregaron claves a terceros la tiene la demandada quien con sus registros debía aportar la información suficiente para establecer que había obrado dentro de todo su cuidado y que la culpa por ende se trasladaba al usuario.

En este caso no fue así pues reitera esta parte que no existe una sola prueba que indique que los token que permitieron la defraudación del municipio de Roncesvalles llegaron a los teléfonos registrados y a los correos registrados y que son los mismos que fueron utilizados para generar los traslados así como para autorizar los mismos.

Revisando el juicioso trabajo de quien representó al banco judicialmente se puede establecer que los registros no fueron aportados al proceso porque precisamente los mismos deben tener situaciones irregulares que no hubieran permitido como se hizo en primer instancia que se trasladará la responsabilidad al municipio de Roncesvalles.

Igualmente si un usuario administrador realizó alguna situación anormal, tuvo que haber demostrado el banco que dicha situación le fue informada al usuario auditor en qué fechas porque canal y a qué hora para determinar que el mismo fue negligente y permitió que se realizaron maniobras que atentaban contra el patrimonio público en cabeza del municipio.

Conclusión de lo expuesto es que el régimen de responsabilidad de los Bancos corresponde a la teoría del «riesgo profesional». En esta última, la obligación de asumir los riesgos inherentes al ejercicio de la actividad se basa en el profesionalismo que esta requiere. Única forma que el banco hubiere podido trasladar la responsabilidad al titular de la cuenta, es que hubiese demostrado que el mismo fue negligente porque las claves utilizadas fueron las que el banco proporcionó y no otras que lo que demostrarían era la vulneración del sistema electrónico de un banco que muchas veces ha sido burlado enseñando sé especialmente contra las entidades públicas en especial los municipios más pequeños del país.

Del señor juez,



ALVARO ANDRES BUITRAGO CADAVID
C.C. 94.410.951 de Cali
T.P. 109.439 del C.S.J.