CERTIFICO: que se anunciaron para alegar, escucharon relación y alegaron, por el recurso, el abogado don Felipe Vega Gómez y el abogado don Juan Manuel Errázuriz, contra el mismo. Santiago, siete de agosto de dos mil diecinueve.

Elizabeth Melero López
Relatora

C.A. de Santiago

Santiago, siete de agosto de dos mil diecinueve.

Vistos y teniendo presente:

Primero: Que don Fernando González Leiva, contador auditor, recurre de protección en contra del Banco Bilbao Vizcaya Argentaria Chile (BBVA), sociedad anónima del giro de su denominación, rol único tributario 97.032.000-8, representada por don Manuel Antonio Olivares Rossetti, argumentando una conculcación al derecho de propiedad que le reconoce la Constitución Política de la República, por el acto que estima arbitrario e ilegal consistente en la negativa del Banco de la devolución de los dineros sustraídos fraudulentamente de su cuenta corriente.

Funda su recurso en el hecho que los días 15 y 16 de Mayo de 2019 supuestos terceros defraudadores, aprovechándose de la fusión entre Scotiabank Chile y BBVA y por ello de la migración de los clientes del BBVA a Scotiabak habrían obteniendo a su nombre un crédito de consumo *online* por $13.600.000, para luego extraer dichos dineros de su cuenta corriente y, además, otros de su línea de crédito por $889.960. En consecuencia se habría generado un "pasivo" en favor del banco por la suma de $14.489.960.- pesos, negándose hasta la fecha a eliminar dicho pasivo de su patrimonio a pesar de reconocer el fraude.

Señala que el día 16 de mayo lo contacta un ejecutivo del banco indicándole que producto del proceso de migración de clientes debía realizar una actualización de sus claves de ingreso a la página web del Banco, para lo cual se le envió a su teléfono celular y a su correo electrónico (información que ellos ya tenían en su poder) las claves para ingresarlas al sitio web, generando una nueva clave única de acceso.

Asimismo, le solicitan digitar en su teléfono celular las claves de su tarjeta de coordenadas, no dándolas verbalmente, sino que digitándolas directamente en el teléfono.

Ese mismo día, le llega un correo electrónico señalándole que la activación en Scotiabank Azul había sido exitosa y que ahora podía realizar transferencias y pagos sin la tarjeta de coordenadas. Y luego a las 23:28 un correo informándole que se había contratado un crédito de consumo. Luego, en la medianoche del día 17 se hacen en menos de 22 minutos desde el otorgamiento del crédito, tres transacciones por $6.929.980 con cargo al crédito de consumo que jamás solicitó. Asimismo, en la madrugada siguen haciendo 10 transacciones más por un total de $6.659.980. Al haberse acabado los fondos, utilizan la línea de crédito por $889.960, por lo que al día 17 de mayo de 2019 tenía un pasivo millonario de $14.489.960, que fue fraudulentamente generado.

Explica que el 17 de mayo a las 8:26 hace la denuncia ante la 17ª Comisaría de Las Condes y luego a una sucursal del banco recurrido para ponerlos en conocimiento de los hechos fraudulentos que había sido víctima.

Sostiene que el banco recurrido reconoce el fraude, pero a pesar de ello se niega a restituir en su patrimonio los efectos del fraude del que fue víctima. Ante las consultas sobre la restitución de los dineros, el 13 de junio le responde un ejecutivo de la sección antifraude, quien le indica que una aseguradora había liberado un cheque a su favor por la suma de $277.545, cifra que no alcanza siquiera a cubrir los intereses del préstamo fraudulento. Indica que este préstamo devenga intereses que benefician al banco recurrido.

Indica que el banco recurrido realiza una serie de actos arbitrarios e ilegales, siendo éstos: a) sin mediar su consentimiento, generó créditos a su favor con cargo a su patrimonio, ya que un tercero on line, bajo su titularidad solicita un préstamo cerca de la medianoche y durante las primeras horas de la madrugada accede a su cuenta corriente e incluso a su línea de crédito, transformando al recurrente en un deudor insolvente y b) se niega a restituir los fondos defraudados o eliminar el pasivo

generado, afectando con ello su derecho a la propiedad. Hace presente que es una práctica comercial habitual el poner de cargo de los cuentahabientes los efectos de los fraudes de los que son víctimas y cita al efecto un fallo de la Excma. Corte Suprema, rol 29.892-2019.

Estima que el actuar del banco recurrido afecta su derecho a la integridad psíquica prevista en el art 19 N°1 de Constitución Política de la República, ya que de un día para otro pasa a ser un deudor insolvente con una deuda millonaria, que sobrepasa con creces el activo de su patrimonio. Asimismo vulnera su derecho a la propiedad previsto en el artículo 19 N°24 de la Carta Fundamental, esto debido a que el banco recurrido al generar sin su consentimiento un pasivo, trasladando a su patrimonio los efectos del fraude del que fue víctima.

Por último, pide que se acoja el recurso, ordenando la disposición de los fondos en la cuenta del actor para solventar el pasivo generado, o bien, derechamente, la eliminación de este pasivo y/o cualquier otra medida que esta Corte estime pertinente.

Acompaña al efecto, los documentos señalados en el primer otrosí de su recurso.

Segundo: Que informa el abogado don Juan Manuel Errázuriz Pomes**,** en representación del recurrido Scotiabank Chile, solicitando el rechazo del recurso.

En primer lugar, señala que existen hechos reconocidos por el actor: 1.- El cliente reconoce haber entregado sus claves directamente a tercero, supuestamente, un ejecutivo lo contactó para “actualizar sus claves” (pese a que es un hecho público, notorio y ampliamente difundido por los Bancos que nunca se llamará a los clientes para pedirles sus claves), enviándose a su correo y a su teléfono dos claves de seguridad, no siendo ésta una práctica habitual de la industria.

2.- En caso de existir un fraude, cuestión que esta parte controvierte, ello se debe única y exclusivamente a que el cliente entregó todas sus claves a un tercero, lo que claramente es una negligencia y a los pocos minutos el banco le envía mi un correo informándole que se había activado la aplicación Scotiabank Azul Pass, en el cual se indica que

puede realizar transferencias y pagos sin su tarjeta de coordenadas y que si no ha realizado dicha operación, puede llamar a un número.

Además, alega que la postura de la Excma. Corte Suprema en casos que los clientes reconocen haber entregado sus claves a terceros, es distinta a la señalada por el recurrente cuando se reconociéndose la entrega de información confidencial a terceros, no puede alegarse una supuesta negligencia de mi representada.

En otro acápite alega que el contrato de cuenta corriente bancaria es un contrato distinto del contrato de depósito irregular, tienen una regulación distinta y de las cuales emanan obligaciones distintas para las partes y la distinta normativa establecida por el ente el regulador, obliga a las instituciones a contar con sistemas y procedimientos de seguridad y a adoptar las medidas de publicidad necesarias para informar sobre la obligación de cuidado mínimo que deben observar los clientes para evitar los fraudes, medias que su parte ha cumplido.

Sostiene que en los contratos de cuenta corriente que los clientes celebran con esa institución, se traslada el riesgo de fraude al cliente en caso que este no adopte las medidas de cuidado debidas respecto de sus claves, esto debido a que el uso y custodia de las claves es responsabilidad de los clientes. De esta forma, no existiendo una vulneración a los sistemas del Banco, de acuerdo a lo pactado, no es responsabilidad de su representada el restituir suma alguna.

Luego explica el funcionamiento de la aplicación “Scotiabank Azul Pass”, que fue el mecanismo utilizado por quienes presuntamente habrían robado los dineros del recurrente, indicando que para la autorización de una transacción con BBVA PASS, inicialmente se requieren no de una, sino de 4 contraseñas y códigos para que la misma fuese activada. Esta es una aplicación segura pues todos los clientes cuentan con un PIN de seguridad de tres dígitos, que eligieron al momento de activar BBVA Pass. Este PIN, que es personal y confidencial, es requerido para generar la clave automática que autoriza las transacciones desde el celular o desde el sitio web.

Además, los clientes del BBVA Chile tiene a disposición otra aplicación adicional llamada “BBVA Wallet”, hoy “Scotiabank Azul Wallet”, la que además de ser una analogía digital de la tradicional billetera, permite recibir notificaciones instantáneas en el móvil de los movimientos realizados con las tarjetas de crédito y débito del banco, lo que permite a los usuarios llevar un control en línea de todas las transacciones de forma eficiente y segura.

En cuanto a los argumentos de derecho realiza una serie de alegaciones para el rechazo del recurso, las que son:

1.- La ley señala que son los tribunales ordinarios de justicia los encargados de determinar los estados de cuenta en caso de diferencias entre las partes;

2.- La acción de protección no procede frente a un supuesto incumplimiento contractual. Se trata, en consecuencia, de un asunto de lato conocimiento y no de una acción cautelar de emergencia.

3.- No existe acto arbitrario o ilegal de Scotiabank Chile, por lo ya señalado precedentemente debido a que son las partes quienes han trasladado el riesgo al cliente en caso de fraudes que se produzcan con motivo de la falta de custodia de la clave personal y datos del cliente.

4.- No existe privación, perturbación o amenaza de un derecho del actor por parte de Scotiabank Chile.

5.- No existen medidas que esta Ilustrísima Corte pueda adoptar, porque no le es posible restituir dineros que no ha recibido, sino que han sido transferidos a terceros, sin vulneración de las medidas de seguridad del Banco, con claves secretas cuya custodia le corresponde a la recurrente.

Tercero: Que el recurso de protección de garantías constitucionales establecido en el artículo 20 de la Constitución Política de la República constituye jurídicamente una acción de evidente carácter cautelar, destinada a amparar el legítimo ejercicio de las garantías y derechos preexistentes que en esa misma disposición se enumeran, mediante la adopción de medidas de resguardo que se deben tomar

ante un acto arbitrario o ilegal que impida, amague o perturbe ese ejercicio.

Cuarto: Que para acoger la presente acción debe constatarse la existencia de un acto arbitrario o ilegal que impida, amague o perturbe el ejercicio de un derecho preexistente e indiscutido.

En efecto, el recurrente sostiene que el Banco no ha podido eximirse de responsabilidad respecto de los hechos que le han afectado, lo que sería consecuencia de manifiestas deficiencias en sus sistemas de seguridad, lo que permitir a terceros acceder ó al dinero que mantenía en su cuenta corriente y girarlo por medio de una operación que desconoce, pero que involucraba el uso de las claves de seguridad que el Banco provee a sus clientes.

Quinto: Que dichas aseveraciones han sido refutadas por la institución recurrida, señalándose por esta que en la operación de transferencia fueron utilizadas las distintas medidas de seguridad debido a que el recurrente instaló la aplicación "Scotiabank Azul Pass", permitiendo de esta forma realizar transferencias y pagos sin necesidad de utilizar su tarjeta de coordenadas, y que de la activación de dicha aplicación, el Banco le dio el debido aviso al recurrente, señalando incluso que si desconocía dicha operación podía llamar a la mesa de ayuda.

Lo anterior permite concluir que se utilizó el canal normal para la operación, y permite descartar una intrusión de los sistemas de seguridad electrónicos.

En cualquier caso, el impugnante no precisa en su libelo cuál de los mecanismos implementados por la recurrida en favor de sus usuarios es el que falló, atribuyéndole responsabilidad en un hecho respecto del cual bien pudo no tener intervención alguna, más aun si los antecedentes aportados por la recurrente nada revelan respecto de la deficiencia en que funda la infracción denunciada.

Sexto: Que de los antecedentes del recurso y los allegados a esta causa, no permiten concluir la existencia de un supuesto incumplimiento de las obligaciones del contrato suscrito entre las partes que pueda ser

reparada por esta acción constitucional, para exigir la devolución del dinero que el recurrente afirma haber salido de su patrimonio de manera irregular.

De esta forma, no se verifica la existencia del primero de los presupuestos exigibles para la procedencia del recurso de protección, cual es la existencia de un acto u omisión arbitrario e ilegal por parte de la recurrida, pues, como ya se dijo, no existe antecedente alguno que dé cuenta de la vulneración de algún sistema de seguridad del banco que haya permitido que terceros, defraudando dichas medidas, hayan obtenido las claves personales del actor, con el propósito de obtener un crédito de consumo on line, para luego, sustraer dicha cantidad mediante una serie de transferencias; sino que, como lo reconoce el propio actor, dichas claves le fueron solicitadas por un tercero que se identificó como ejecutivo del banco y que él accedió a modificar su clave, digitándola directamente en su teléfono celular, lo que involucraba el uso de las claves de seguridad que el Banco provee a sus clientes.

Séptimo: Que a mayor abundamiento, de los antecedentes que han sido expuestos aparece con claridad que se han discutido cuestiones de hecho cuyo esclarecimiento excede los márgenes de aplicación del presente recurso de protección. Así las cosas, resulta notorio que el recurrente carece de un derecho indiscutido y preexistente de aquellos cuyo imperio esta Corte debe proteger, razón suficiente para concluir que la presente acción ha de ser desestimada.

Por estas consideraciones y de conformidad con lo que dispone el artículo 20 de la Constitución Política de la República y el Auto Acordado de esta Corte sobre la materia, se rechaza el recurso de protección deducido por don Fernando González Leiva.

Acordada con el voto en contra del Ministro señor Jorge Zepeda Arancibia, quien fue del parecer de acoger el recurso, fundado en que la maquinación fraudulenta se efectuó con el uso de aparatos propios del Banco, que son entregados al cliente para permitirle la operación de su cuenta corriente mediante medios informáticos, por lo que la correcta

operación y seguridad en los mismos le resulta imputable a la recurrida, y resulta responsable de su vulneración.

Asimismo, la transferencia fue efectuada sobre fondos del cuenta correntista, entregados en depósito a la recurrida, y para efectuar la operación se requirió el uso de información entregada por el cliente al Banco, de lo que se colige en forma inequívoca que se obtuvieron por una falla ostensible de la recurrida en su deber de confidencialidad.

Por lo expuesto, estima que se han vulnerado las garantías fundamentales del artículo 19 N°24 de la Constitución del recurrente, causándole un perjuicio por $14.489.960.-

Regístrese y comuníquese.

N°Protección-49111-2019.

JUAN MANUEL MUÑOZ PARDO
Ministro
Fecha: 07/08/2019 13:15:39

JORGE LUIS ZEPEDA ARANCIBIA
Ministro
Fecha: 07/08/2019 13:15:40

MARIA CECILIA DEL PILAR RAMIREZ GUZMAN
ABOGADO
Fecha: 07/08/2019 13:11:34

Pronunciado por la Undécima Sala de la C.A. de Santiago integrada por los Ministros (as) Juan Manuel Muñoz P., Jorge Luis Zepeda A. y Abogada Integrante Maria Cecilia Ramirez G. Santiago, siete de agosto de dos mil diecinueve.

En Santiago, a siete de agosto de dos mil diecinueve, notifiqué en Secretaría por el Estado Diario la resolución precedente.

KGHEJFXPMW