C.A. de Santiago

Santiago, diez de diciembre de dos mil diecinueve.

Al folio 547006: téngase presente.

Vistos y teniendo presente:

PRIMERO: Que comparece David Brito Hevia, abogado, quien interpone recurso de protección en favor de DANIELA VIVIANS ROJAS VIVANCO, ingeniera, ambos con domicilio para estos efectos en Huérfanos 1022, oficina 1405, comuna de Santiago, en contra del BANCO SANTANDER-CHILE, por el acto que estima arbitrario ilegal consistente en no restituir fondos que habrían sido sustraídos ilegítimamente desde su cuenta corriente.

Funda su recurso en que Daniela Vivians Rojas Vivanco, posee hace más de 5 años diversos productos comerciales con el Banco Santander-Chile.

Indica que durante el mes de septiembre del año en curso, mientras efectuaba la revisión de sus finanzas en la plataforma informática del banco, una vez que accede al sistema, previa digitación de su RUT y clave secreta, se le indica que debe registrar 3 pares de coordenadas de su tarjeta de transferencias electrónicas (denominada SuperClave) por razones de seguridad informática. Una vez realizado esto, pudo verificar el estado de sus finanzas.

Posteriormente, luego de algunos minutos, recibe diversas notificaciones a su teléfono celular, respecto de que se habían realizado 8 transferencias a destinatarios desconocidos, por un total de $2.000.000.-

Indica que el día de las transacciones, no se registran envíos de correos electrónicos a la casilla de la titular, así como la nula solicitud de alguna clave extra, la cual sería común cuando se producen giros de

dineros por altas sumas, como sucede en el caso de marras. Solamente proporcionó la información correspondiente a 3 pares de dígitos, una vez que ingresó a la plataforma de internet de la propia institución.

En virtud de lo anterior, la recurrente interpuso un reclamo ante el Banco Santander-Chile, el mismo día en que acecen los hechos, donde explica los eventos sucedidos, así como los fundamentos para solicitar la restitución de los dineros girados, como también todos los gastos derivados del uso de los productos.

Posteriormente, el 11 de octubre, el banco remite vía electrónica, un Informe de Liquidación, de Zurich Santander Seguros Generales N° 202069, respecto del siniestro N° 219040085, en que realiza un análisis de la póliza de seguros POL 120130503, en la que procede a realizar un análisis de la Cobertura, que determina que la cantidad indemnizable asciende a la cantidad de $1.542.053.-, ya que el monto máximo de la indemnización y agregado anual de la póliza invocada asciende a UF 55,00.

Agrega que es un hecho público y notorio que durante el último año se han producido una serie de fraudes informáticos que han acarreado una serie de gastos realizados sin la autorización de los usuarios de los productos bancarios. Lo anterior daría cuenta, de manera inequívoca, que no existe voluntad alguna por parte de la reclamante de realizar transacción alguna y, a contrario sensu, se permite afirmar que las transacciones ejecutada sin el consentimiento, conocimiento y autorización de esta.

A juicio del recurrente, el actuar de la entidad bancaria recurrida, en torno a sostener su negativa de reintegrar la totalidad de lo sustraído, constituye un acto ilegal y arbitrario que conculca el derecho de propiedad de la recurrente.

Agrega que las claves de acceso, tarjetas de coordenadas, terceras claves, sitio web, aplicación móvil, etc., son diseñadas,

elaboradas y proporcionadas por el banco, por lo que sería contrario a derecho y a la lógica que la reclamante deba asumir el riesgo de una actividad cuyo control es del requerido.

Respecto del vínculo contractual y la obligación de la recurrida de restituir los fondos sustraídos mediante fraude informático estima que es innegable la obligación que tienen los bancos e instituciones financieras de garantizar la seguridad de las transacciones que el mismo banco autoriza por cualquiera de los medios ofrecidos al público, con independencia de si los dineros sustraídos provienen de cuentas de ahorro o de cuentas corrientes.

Agrega que al vulnerarse los sistemas de seguridad del banco o la empresa externa que brinda el servicio, la responsabilidad por este tipo de defraudaciones recae directamente en la institución bancaria, quien, por negligencia, no ha adoptado las medidas de seguridad suficientes para evitar el acceso de defraudadores que afecten el patrimonio de sus clientes, incumpliendo la obligación esencial de este tipo de contratos. En este sentido, los clientes no pueden asumir la carga por este tipo de riesgos.

Adiciona que la obligación principal y esencial del Banco, es la restitución de las sumas depositadas, esto es, la misma cantidad de dinero que ha recibido, y como se trata un depósito de cosas fungibles, la propiedad de estas pasa al Banco, debiendo, como ya se mencionó, restituir las sumas de dinero equivalentes.

Solicita en definitiva que se haga devolución o restitución de los dineros sustraídos de la Cuenta Corriente, Tarjeta de Crédito y Línea de Crédito de su parte, esto es, $457.947, más los intereses, reajustes y multas que se le haya cursado por la institución financiera, o la cantidad mayor o menor que este tribunal determine, con costas.

SEGUNDO: Que en su informe, la recurrida Banco Santander solicita el rechazo del presente recurso.

Indica que no es efectivo que haya existido una vulneración de los sistemas de seguridad del Banco Santander Chile, ni menos que ésta se haya verificado al interior de su plataforma web.

Así habría quedado establecido de la investigación interna que el Banco llevó a efecto en su Departamento de Fraudes Electrónicos, área técnica y especializada en estas materias, luego de ingresado el reclamo de la recurrente.

Indica que de los propios dichos de la recurrente se desprende que no accedió a página web del banco sino que a otra que podía ser muy parecida, pues jamás el banco le habría solicitado los números de su tarjeta Súper clave para revisar su cuenta. La recurrente reconoce que hace más de cinco años opera sus productos a través de los sistemas digitales del banco, por ende no puede alegar ignorancia sobre este punto.

A juicio del banco, al entregar la recurrente la información, ella comprometió su clave y eso fue lo que permitió que terceros extraños pudieran luego extraer de su cuenta las sumas reclamadas, cuestión que escapa de la responsabilidad del banco.

Estima que es necesario tener presente que los sistemas de seguridad que provee el Banco Santander Chile, así como cualquiera otra institución bancaria, para el uso electrónico de los productos que ofrece, están estandarizados en el sistema financiero y son regulados por la Superintendencia de Bancos.

En particular, el Banco Santander Chile ha implementado un sistema de seguridad para acceder electrónicamente a través de su página web a las cuentas corrientes y efectuar operaciones en ella:

1) Clave secreta: Esta es la clave que el propio usuario determina y permite el acceso electrónico a la cuenta corriente a través de la página web del Banco Santander Chile.

2) Súper Clave: Esta se obtiene a partir de una tarjeta que el banco entrega al usuario al momento de contratar una cuenta corriente, la que contiene hasta 50 números distintos que se pueden relacionar aleatoriamente mediante coordenadas.
3) Clave 3.0: Esta clave es exigida por el Banco para determinadas operaciones que involucran transferencias a terceros ya conocidos de sumas de dinero más altas de lo habitual o por cualquier suma a terceros desconocidos que no hayan sido antes destinatarios de fondos.

Sobre este particular, en el caso de autos, el informe técnico de Departamento de Fraudes del banco pudo constatar que en la investigación interna del banco se pudo establecer que se instruyeron aparentemente por la titular de la cuenta diversas transferencias desde su cuenta corriente a terceros no habituales. Siendo así, para darles curso fue necesario entonces requerir las tres claves de seguridad, y solo ingresadas correctamente las mismas pudo llevarse a efecto las transacciones que la actora reclama.

Se concluyó en la investigación en comento que "…las transacciones reclamadas fueron ejecutadas con todos los mecanismos de seguridad del Sistema Home Banking, en este caso: aplicativo Santander Pass y de que no existe o se evidencia vulneración alguna de los sistemas de seguridad y estándares o procedimientos del banco, certificamos el caso como ¨Troyano en el equipo del cliente¨ (el subrayado es nuestro).

Por ello, concluye el recurrido, que de haber existido el fraude, este necesariamente debió materializarse en el sistema computacional de la actora y en su línea telefónica, permitiendo el conocimiento y manipulación por parte de terceros de su información personal y confidencial y la utilización de sus productos de uso exclusivo y personal, lo que permitió que la operación fuera recibida por el banco como legítima. Normalmente esto tiene lugar porque los usuarios

ingresan a páginas falsas que no pertenecen al banco por su propia desidia, negligencia o descuido, de las cuales son capturados sus datos que luego permiten ingresar correctamente al sistema del Banco.

Agrega la recurrente omite señalar el hecho substancial de que, gracias a la oportuna intervención del banco, luego de efectuada la denuncia, se logró retener la suma de $ 450.000 de la cuenta receptora de los fondos defraudados existentes en el Banco Estado. No obstante, el banco no ha sido informado de que la recurrente haya realizado ante el banco citado, las gestiones destinadas a obtener la restitución de estos fondos, pues es a ella a quien le corresponde efectuar esta diligencia. Lo relevante, para efectos de este recurso, es que estos fondos están disponibles para la recurrente y solo depende de su diligencia obtener su restitución. Tales fondos son equivalentes a la suma reclamada por esta vía a mi parte, lo que no se justifica de modo alguno atendida esta circunstancia.

De todo lo expuesto, derivaría la imposibilidad de asignar responsabilidad alguna al banco en los hechos reclamados. Ello además porque al momento de contratar estos servicios, la recurrente suscribió con fecha 28 de diciembre de 2015 el “Contrato de Plan de Servicios Financieros” que incorpora “Las Condiciones Comunes del Contrato para Operar a través de Cajeros Automáticos y demás Medios Electrónicos o Sistemas Bancarios Automatizados y Remotos”, el cual establece en el punto B referido a Acceso y Operación de los sistemas, lo siguiente:

“1. Para tener acceso y operar los Servicios Automatizados el Cliente deberá utilizar los procedimientos y/o medios de seguridad, identificación e integridad que el Banco ha implementado o implemente en el futuro, para cada uno de ellos, y que pudieren estar asociados a los elementos requeridos para su utilización, tales como tarjetas magnéticas, número de RUT y/u otros. Entre ellos figuran los códigos o

claves secretas, firmas electrónicas. Avanzadas o no, y cualesquier otro mecanismo de seguridad de acceso y/u operativo que el Banco o los operadores de los SISTEMAS AUTOMATIZADOS hubiesen establecido o establezcan en el futuro, en adelante la Firma Electrónica".

Consistente con lo anterior en él. 12.4 del contrato, en relación a la firma electrónica, las partes establecieron lo siguiente:

"El Cliente ha sido informado, entiende y acepta asimilar jurídicamente las claves secretas o firmas electrónicas que el Banco le proporcione, incluidas su PIN de Tarjeta de Crédito, a su firma manuscrita y consiente el que ésta debe ser secreta, personal e intransferible, por lo que el Cliente se obliga a mantener la debida diligencia, sigilo y cuidado en su utilización, asumiendo la responsabilidad por los perjuicios que el mal uso o la utilización errónea de la firma electrónica y o de los servicios automatizados, pueda ocasionarle al mismo Cliente, al Banco y o a terceros, cuando dicha mal utilización les sea imputable a éste".

En consecuencia, desde el mismo inicio de la relación contractual entre el cliente y el banco queda determinado por la ley del contrato que la responsabilidad en el uso, resguardo, custodia y confidencialidad de la clave personal queda en manos exclusivas del usuario.

Adiciona que el banco no ha podido dejar de cursar las operaciones reclamadas sin incurrir en una infracción legal y reglamentaria, ello porque una vez cumplidos los requisitos para que operaran las transferencias cuestionadas por la recurrente, esto es, una vez ingresadas correctamente las tres claves de seguridad en este caso a la plataforma verdadera del banco, éste no podía sino cumplir con su obligación legal de dar curso a dichas órdenes de transferencia que había recibido, según entendía, del titular de la cuenta, puesto que las claves que debían estar en su solo conocimiento fueron correctamente ingresadas al sistema para este efecto.

Según los antecedentes a que ha tenido acceso el banco, no existía indicio alguno de patrón de fraude que pudiere haberse detectado con antelación a las transferencias efectuadas, Por el contrario, ha podido confirmarse internamente que operaron todas las medidas de seguridad y que se respetaron y aplicaron en cada caso los procedimientos determinados para las operaciones de este tipo.

Recalca que las instituciones financieras previenen en forma permanente y reiterada a sus clientes en los mismos soportes de internet del riesgo de no acceder en la forma correcta a la plataforma de la respectiva institución bancaria y de la existencia de estas páginas falsas que pueden exponerlos a riesgos de fraude.

En particular, el acceso a estas páginas falsas permite el fraude cibernético conocido como Phishing y a ellas los usuarios no acceden a través de la dirección que da el banco, sino por una vía alternativa más corta y no autorizada, simplemente por la mera desidia de querer ahorrarse la digitación del nombre completo de la página oficial del Banco, lo que puede acarrear nefastas consecuencias como las que hoy dice lamentar la recurrente.

Finalmente destaca que luego de efectuada la denuncia por parte de la señora Rojas, se logró retener la suma de $ 450.000 de la cuenta receptora de los fondos defraudados existentes en el Banco Estado. Estos fondos están disponibles para la recurrente y solo depende de su diligencia obtener su restitución, pues es a ella como titular de la cuenta corriente afectada por el delito de fraude es a quien le corresponde efectuar esta diligencia.

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 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 ésta que en las operación de transferencia fueron utilizadas las distintas medidas de seguridad debido a que el recurrente ingresó correctamente sus coordenadas de seguridad, permitiendo de esta forma realizar transferencias y pagos.

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 realizar una serie de transferencias; sino que, como lo reconoce el propio actor, dichas claves le fueron ingresadas voluntariamente por la recurrente en la plataforma virtual que a su juicio correspondía a la del Banco Santander, 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 la Excma. Corte Suprema sobre tra, **se rechaza** el recurso de protección deducido en favor de Daniela Vivian Rojas Vivanco.

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 perjuicio patrimonial.

Regístrese y comuníquese.

N°Protección-162853-2019.

Pronunciada por la **Undécima Sala** de esta Corte de Apelaciones de Santiago, presidida por el Ministro señor Juan Manuel Muñoz Pardo e integrada por el Ministro señor Jorge Zepeda Arancibia y por el Abogado integrante señor Cristian Lepin Molina.

JUAN MANUEL MUÑOZ PARDO
MINISTRO(P)
Fecha: 10/12/2019 12:16:03

JORGE LUIS ZEPEDA ARANCIBIA
MINISTRO
Fecha: 10/12/2019 12:09:52

CRISTIAN LUIS LEPIN MOLINA
ABOGADO
Fecha: 10/12/2019 12:15:06

Pronunciado por la Undécima Sala de la C.A. de Santiago integrada por Ministro Presidente Juan Manuel Muñoz P., Ministro Jorge Luis Zepeda A. y Abogado Integrante Cristian Luis Lepin M. Santiago, diez de diciembre de dos mil diecinueve.

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