Exp. 11-005470-1027-CA
Res. 000686-F-S1-2014

SALA PRIMERA DE LA CORTE SUPREMA DE JUSTICIA. San José, a las nueve horas quince minutos del veintiocho de mayo de dos mil catorce.

Proceso de conocimiento establecido en el Tribunal Contencioso Administrativo y Civil de Hacienda por **OPTOMEL SOCIEDAD ANÓNIMA**, representado por su representante legal Enmanuel Barrientos Valverde, soltero, optometrista; contra el **BANCO DE COSTA RICA**, representada por su apoderado general judicial, Alejandro Faba Alpizar, no indica calidades, ni domicilio. Figuran como apoderados especiales judiciales, de la parte actora, Juan José Nassar Güell, Ricardo José Nassar Güell, soltero; por el ente demandado, Helberth Obando Durán. Las personas físicas son mayores de edad, vecinos de San José, y con las salvedades hechas, casados y abogados.

RESULTANDO

1.- Con base en los hechos que expuso y disposiciones legales que citó, el actor estableció proceso de conocimiento, para que en sentencia se declare: *"1. ...la nulidad de lapresunción de culpabilidad del usuario por el uso del PIN o clave secreta en operaciones fraudulentas, que consta en el procedimiento administrativo, por vulnerar los derechos de los consumidores. 2. Que se condene al Banco de Costa Rica a aceptar la responsabilidad por la estafa electrónica que sufrimos los suscritos ypor ende se nos indemnice con lo susttraído, sea la suma de cuatro millones seiscientos mil colones. 3. Que se condene al Banco de Costa Rica al*

pago de daños y perjuicios en abstracto, por hacer caso omiso a los institutos internacionales ya (sic) *los sistemas de protección de ususarios, así como desinformar a los mismos de los delitos electrónicos, mismos que solicito se fijen po medio de perito actuarial en su momento procesal oportuno. 4. Que se declare la nulidad del reglamento para servicios de banca electrónica del Banco de Costa Rica, por ser abusivo y contrario al derecho costarricense, y se le obligue al banco a emitir nuevo reglamento de acuerdo a la legislación vigente y la equidad y el buen derecho. 5. que* (sic) *se obligue a los bancos a entregar una copia de los contratos de adhesión de los servicios de la banca electrónica a cada cliente. 6. Se condene a la entidad bancaria demandada al pago de ambas costas procesales así como a los honorarios profesionales generados en el presente proceso."*

2.- El apoderado de la parte demandada contestó negativamente e interpuso las excepciones de falta de derecho y falta de legitimación activa y pasiva.

3.- Al ser las 8 horas del 23 de mayo de 2012 se efectuó la audiencia preliminar, oportunidad en que hicieron uso de la palabra los representantes de ambas partes.

4.- El Tribunal Contencioso Administrativo, Sección Cuarta, integrada por la Juez Grace Loaiza Sánchez y los Jueces Ricardo Madrigal Jiménez y Francisco Muñoz Chacón, en sentencia no. 090-2012 de las 12 horas del 31 de agosto de 2012, resolvió: *"Con las aclaraciones realizadas se rechaza las defensas de falta de legitimación pasiva. De oficio se declara la falta de interés con respecto a la pretensión de nulidad del Reglamento de Banca Electrónica del Banco de Costa Rica. Se rechazan las excepciones de culpa de la víctima y hecho de un tercero. Se rechaza parcialmente la excepción de falta de derecho, entendiéndose aceptada en todo aquello que no se he otorgado expresamente. Se declara parcialmente con lugar la demanda, y se condena al*

Banco de Costa Rica, en los siguientes términos: 1) Se ordena reintegrarle a los actores Optomel S.A. y Emmanuel (sic) *Barrientos Valverde, la suma total de TRES MILLONES SETECIENTOS MIL COLONES; por concepto de daño material; 2) La suma concedida por daño material deberá ser indexada de conformidad con el numeral ciento veintitrés del Código Procesal Contencioso Administrativo, desde la sustracción hasta la firmeza de este fallo; 3) Debe el Banco sobre la suma dicha canelar los intereses de conformidad con el numeral mil ciento sesenta y tres del Código Civil desde la firmeza del fallo hasta su efectivo pago y 4) Se condena a la parte demandada al pago de las costas procesales y personales de este asunto. 2) Estos últimos tres rubros deberán liquidarse en ejecución de sentencia. 6) Se ordena al Banco de Costa Rica a entregarle y explicarle al actor los alcances concretos de los contratos que lo unen a partir de las cuentas que este último tiene con la institución bancaria; incluyendo la entrega de copia de los documentos."*

5.- El apoderado del Banco formula recurso de casación indicando las razones en que se apoya para refutar la tesis del Tribunal.

6.- En los procedimientos ante esta Sala se han observado las prescripciones de ley. Participa en la decisión de este asunto el magistrado suplente López González.

Redacta el magistrado González Camacho

CONSIDERANDO

I.- De los hechos probados y no controvertidos en el fallo del Tribunal, así como de la prueba allegada a los autos, se tiene que Optomel Sociedad Anónima (en adelante Optomel) y el señor Emmanuel Barrientos Valverde son titulares de cuentas en el Banco de Costa Rica. La primera, de la cuenta corriente no. 001-281074-3. El segundo, de la cuenta de ahorros no.

001-510490-4. En ambas cuentas, se encuentra autorizado don Emmanuel. En fecha 13 de octubre de 2007, el último se afilió al servicio “bancoBCR.com”, que es un sistema de banca electrónica. El contrato electrónico que permite dicha afiliación y que debe ser aceptado para ingresar y utilizar el sistema, establece la obligación de los clientes de no entregar los datos de la clave dinámica. Este mecanismo o dispositivo de seguridad permite múltiples combinaciones de datos en tríadas, lo que dificulta su vulneración si no se cuenta con los valores que consigna. El Banco efectuó una campaña televisiva, radial e impresa sobre la importancia de no entregar los datos que ésta consigna. El 3 de diciembre de 2008, don Emmanuel obtuvo la clave dinámica 413-FC1F5-9, la cual activó el día 15 siguiente. Dentro de las instrucciones del instrumento se encuentra que sólo el beneficiario puede detentarla y que no debe suministrarla a persona alguna. En junio de 2011, la página de la entidad presentaba como instrumentos de seguridad la inclusión del número de cédula, la clave personal y la clave dinámica. En esa misma época circuló un correo cuyo fin era sustraer la información de los clientes. En fecha 21 de junio de 2011, se realizó una transferencia electrónica de la cuenta corriente 001-0281074-3 de la sociedad, por el monto de ¢1.200.000,00, a la cuenta destino BAC 10200009117759893 del señor Fernando Ortega Calderón, con uso de la clave dinámica 413-FC1F5-9, dirección IP 187.176.172.97. El día 22 siguiente, se efectuó una primera transacción de la cuenta de ahorros 001-510490-4 del señor Barrientos, por la suma de ¢1.500.000,00; y una segunda, de la cuenta corriente 001-0281074-3 de Optomel, por el importe de ¢1.000.000,00; ambas a la cuenta destino BAC 10200009117759893 de titularidad ya señalada, con la misma clave dinámica y a la misma dirección IP. En las tres transacciones se validaron las tripletas del dispositivo de seguridad. En data 23 de junio, el señor Barrientos estableció reclamo ante el Banco de Costa

Rica, por las operaciones que no fueron autorizadas por él; al efecto manifestó que el día 22 anterior, cuando intentó revisar sus cuentas, notó no podía ingresar a la página, pues cuando digitó su clave para la oficina virtual, el sistema le pidió ingresar todos los números de su clave dinámica, lo cual hizo, a lo que la página indicó que la información era errónea; hizo dos intentos adicionales cuyo resultado fue el mismo. Asevera que en horas de la tarde llamó al Banco para verificar si había algún problema, momento en el cual se le indicó podría tratarse de un intento de fraude, por lo que la entidad bloqueó la clave dinámica y el acceso a la página bancobcr.com; y –por último- se percató de la sustracción de ¢3.700.000,00 ese mismo día 23 de junio. En esa fecha, presentó denuncia ante el Organismo de Investigación Judicial (OIJ), donde declaró que al ingresar a la página, ésta era de un hacker, quien tomó sus datos, para luego acceder a sus cuentas y realizar las transacciones. El Banco de Costa Rica comunicó la denuncia a Bac San José, quien congeló el monto de ¢225.000,00. El informe de investigación del 12 de julio de 2011, recomendó no reconocer el reclamo. Mediante nota del 19 de julio de 2011, el Gerente Comercial de Paseo Colón, denegó el reclamo con base en el "*Reglamento de Servicios Electrónicos*", al estimar que las transferencias se realizaron con el usuario, la clave y las coordenadas correctas de clave dinámica. En escrito de fecha 3 de agosto de 2011, ante los recursos de revocatoria y apelación en subsidio planteados, mantuvo la denegatoria y admitió el recurso ante la Gerencia General, quien lo rechazó mediante resolución del 11 del mismo mes. Además, para la resolución de este recurso, resulta de importancia que los sistemas informáticos del Banco no fueron vulnerados, y que existen medios electrónicos que permiten duplicar la página con similitud, apariencia de ser la misma, cuya falsedad se puede determinar

por la dirección electrónica y los mecanismos de seguridad que muestra la página oficial (certificado).

II.- En virtud de lo anterior, Optomel S.A. y Emmanuel Barrientos Valverde demandaron al Banco de Costa Rica para que en sentencia se: 1) declare la nulidad de la presunción de culpabilidad del usuario por el uso del pin o clave secreta en operaciones fraudulentas y del reglamento para servicios de banca electrónica; y 2) obligue al Banco a: 2.1) emitir un nuevo reglamento; 2.2) entregar copia de los contratos de adhesión de servicio de banca electrónica; 2.3) indemnizar: 2.3.1) la suma de ¢3.7000.000,00 que les fue sustraída, y 2.3.2) los daños y perjuicios en abstracto; y 3) pagar ambas costas del proceso. La entidad bancaria se opuso a la demanda y formuló las excepciones de falta de: legitimación en sus dos modalidades y derecho, en particular la culpa de la víctima y hecho de un tercero. El Tribunal denegó la falta de legitimación activa y pasiva. De oficio declaró falta de interés respecto de la pretensión de nulidad del reglamento. Rechazó la culpa de la víctima y hecho de un tercero. Acogió parcialmente la falta de derecho. Declaró con lugar la demanda en forma parcial y ordenó al Banco de Costa Rica: 1) entregar y explicar a la parte actora los alcances concretos de los contratos que les unen en razón de sus cuentas, así como a darle copia; 2) reintegrar la suma de ¢3.700.000,00, 3) cancelar los intereses sobre ese monto desde la firmeza del fallo hasta su efectivo pago, y su indexación desde la sustracción hasta la firmeza; 4) sufragar las costas personales y procesales. Inconforme, el Banco establece recurso de casación, que fue admitido por esta Sala.

III.- En el apartado "*II.- Indebida valoración de la Prueba*", arguye el casacionista que el fallo desatiende la prueba pericial y la participación del testigo perito Leihman Garita Rodríguez,

las cuales demuestran que las transacciones fueron realizadas por un tercero y con información numérica de la clave dinámica, que fue suministrada por los demandantes. Añade, también se pretirió las manifestaciones del señor Barrientos Valverde, primero, ante su Contraloría de Servicios, visibles a folios 2 y 4 del expediente administrativo, donde señala que los días 21 y 22 de junio de 2011, cuando ingresó a la Banca de Personas, se desplegó una página falsa en donde le solicitaron verificar e ingresar todos los números de la tarjeta clave dinámica, lo que el Banco ha insistido no solicitaría; y en segundo lugar, ante el Organismo de Investigación Judicial, a folios 7 y 8 del libelo administrativo de la misma Contraloría, en el sentido de que cuando ingresó a la página "*dicha página era de un jacker,*(sic) *el cual tomó los datos de la misma, para luego poder acceder a mis cuentas y hacer dichas transacciones*". Acota, el Tribunal aceptó que los movimientos fueron realizados por terceros, pero no analizó cómo dichas personas tuvieron acceso a la información completa que les permitió actuar de esa forma, partió de un concepto de responsabilidad objetiva superficial y complaciente con la parte actora, ignorando el debido cuidado en el manejo de la información y la intervención de terceros. Todo lo cual, continúa, violenta los artículos 318 del Código Procesal Civil (CPC) y 82.4 del Código Procesal Contencioso Administrativo (CPCA). Detalla, el testigo perito y la pericia, explican cómo funciona el sistema de doble autenticación, el cual es confiable y que los sistemas de seguridad del Banco no fueron violados. Con lo que se entiende que la única forma de ingresar "*es darle la llave de sistema que permite mediante un procedimiento hacer transacciones*". Por el contrario, asevera, el Tribunal tuvo por no demostrado que el Banco cuente con sistemas de seguridad que le alerten de situaciones irregulares conforme con el perfil del cliente. Prosigue, también tuvo por no acreditado que la entidad fuese ajena al daño y al riesgo, no obstante, comprobó que

implementó la tecnología más adecuada y buscó en el mercado la opción más segura, cual es el sistema de doble autenticación. Bajo el título "*III.- Otras Consideraciones sobre la Infalibilidad del Sistema*", detalla, la única forma posible de ingresar al sitio web es con la clave secreta suministrada al cliente, y dentro de la página es obligatorio para realizar transferencias de fondos el uso de la clave dinámica, la cual se da al cliente en forma física. Afirma, técnicamente no es posible vulnerar la tarjeta de clave dinámica, excepto cuando, por razones claramente ajenas al Banco y provocadas por terceros, la falta al deber de cuidado de los clientes hace que terceros obtengan esa información. Acota, el Banco desde hace varios años ha venido señalando en distintos medios de comunicación la existencia de fraudes informáticos, también en la página web hay recomendaciones, sugerencias y cursos virtuales para que los clientes y visitantes no sean objeto de estafas electrónicas. Incluso en los primeros meses de 2008 se brindó de modo gratuito la clave dinámica, y en forma obligatoria se pidió a partir de setiembre de ese mismo año, de manera que la denominación hackers no es nueva y se conoce popularmente desde hace varios años. Añade, dictó un Reglamento de Servicio de Banca Electrónica, que según los mecanismos del sitio web, debe confirmarse su lectura antes de afiliarse en línea al sistema, y se recomienda al principio de ese procedimiento en línea no realizarlo en sitios o equipos considerados inseguros, como los café Internet, PC's de acceso de otros usuarios, ni redes inalámbricas de acceso público. Agrega, en el mundo virtual, quienes navegan deben tener condiciones mínimas de seguridad, que les permitan navegar e interactuar sin riesgo. Prosigue, en todo momento las transacciones en el sitio web del Banco son autorizadas por los clientes con sus claves secretas, entre ellas el dispositivo físico aleatorio llamado clave dinámica, se utiliza un doble mecanismo de seguridad o autenticación, con el fin de evitar la suplantación de

la identidad, combinando entonces la seguridad virtual o clave de acceso con ese dispositivo físico que se encuentra en custodia y responsabilidad del cliente. Explica, el fraude, electrónico o no, lo que busca es engañar para obtener información valiosa y personal del individuo, en el caso particular la sustracción consciente, inconsciente, directa o indirecta, de la clave de acceso; de esta manera, el Reglamento no es arbitrario, sino consecuencia lógica de una actuación permisiva e imprudente del cliente al suministrar cada dígito y su combinación entre filas columnas, números y letras; el cliente conoce su existencia y alcances. Asevera, la banca electrónica es un medio totalmente seguro cuando se utiliza correctamente. Comenta, entre sus actuaciones están la conferencia de prensa del 6 de diciembre de 2007 sobre este tema, la campaña sobre el uso gratuito y voluntario de la clave dinámica en 2007 y 2008 y su lanzamiento oficial, las pautas en prensa y radio, así como la campaña conjunta con el Banco Nacional de Costa Rica, sobre el fraude electrónico, que se pautó en televisión, radio y prensa. Expone, la clave de acceso y la tarjeta dinámica son secretas y el cliente debe custodiarlas, si por el contrario, consciente o inconscientemente las facilita, debe asumir la responsabilidad de las consecuencias dañosas de sus propios actos. Puntualiza, los fraudes no se producen en su sistema informático, sino que tienen como punto de partida la suplantación o apropiación de la identidad mediante la obtención no autorizada de las claves de acceso; en este caso, de todos los dígitos y combinaciones de la clave dinámica, es decir, los hechos previos al fraude, se producen fuera del sitio web del Banco, en sitios inseguros parecidos, todo esto mientras el usuario navega por Internet, abriendo mensajes, visitando páginas, interactuando, bajando música, video y fotos en sitios inseguros que albergan troyanos, virus, spam y otros mecanismos que obtienen su información. Indica, éstos pueden combatirse con seguir las instrucciones

sencillas mencionadas antes, con tener un antivirus, antispam, muros de fuego y procurar sus actualizaciones periódicas, a lo que se suma el ofrecimiento de otras herramientas como la autorización de transacciones directamente en su sitio web con la clave dinámica. Argumenta, el servicio de banca en línea tiene por fin ofrecer un valor agregado en beneficio de los clientes, quienes voluntariamente aceptan el servicio y sus condiciones y evitan así tener que desplazarse desde su casa u oficina a una sucursal física. Enfatiza, ha hecho esfuerzos encomiables en la implementación de una adecuada plataforma tecnológica, adoptando estándares internacionales de seguridad en los sistemas, con el interés prioritario de garantizar confidencialidad a los clientes, la información no está a disposición de terceros. La encriptación en las comunicaciones, los filtros, los antivirus, la organización sólida en el área de tecnología, son muestras de una administración e identificación apropiada del riesgo. Enuncia, dentro de los controles cuenta con firewall, equipos IPS que detectan y detienen ataques, sistemas de antivirus y antiespías que evitan contagio de sofware maligno, uso de DMZ o zonas de acceso restringido con diferentes niveles de control y que protegen en mayor nivel las bases de datos, sistema de alarma, análisis de vulnerabilidad y parcheo de equipos que garantizan su seguridad, monitoreo externo diario para detectar vulnerabilidades, encriptación, controles a nivel de aplicación y sistema de firma digital. Apunta, la sentencia excluye el deber de cuidado de la parte actora e ignora la culpa de la víctima al entregar la información a un tercero ajeno, permitiendo el acceso a sus fondos, y no indica tampoco qué otro mecanismo debía implementar para que ese daño le fuese ajeno. Todo lo cual, dice, se aparta de lo manifestado por el testigo perito de que lo que se persigue es dar mayor seguridad a los clientes, siempre y cuando éstos sean conscientes de las consecuencias de sus actuaciones en la plataforma, pues

se requiere el manejo seguro de información o llave de acceso. Continúa, el fallo no analiza el sistema de clave dinámica, las publicaciones, recomendaciones ni el curso virtual existente, cuestionándole sin indicar razones o cuál sería un mejor sistema. Asevera, si bien tuvo por acreditado que los días 21 y 22 de junio de 2011, el actor digitó la totalidad de la clave dinámica, luego lo omite, no valora los folios 2 y 4 del expediente de la Contraloría de Servicios ni el peritaje de seguridad, y concluye luego en el hecho no probado 12 que en realidad no cuenta con sistemas de seguridad que le alerten de situaciones irregulares conforme al perfil del cliente. Además, el Tribunal fue más allá, pues tuvo por no probado la forma específica en que los terceros obtuvieron la información de la clave de seguridad y de la tarjeta dinámica, pero acepta que las transacciones fueron realizadas en una dirección IP de la ciudad de México, lo que demuestra que no hay funcionamiento anormal suyo, que es ajeno al daño. Sostiene, afirmaron los juzgadores que no se acreditó que la parte actora conociera los mecanismos de seguridad de su página electrónica, para que pudiese distinguir cuál era real y cuál falso. Explica, esta es una situación similar, análoga a la del cuenta correntista con las fórmulas de cheque; cita parcialmente la sentencia no. 18-2007 del Tribunal Contencioso Administrativo. En este caso, señala, la parte actora no le dio aviso inmediato cuando recibió el correo electrónico, los días 21 y 22 de junio de 2011, sino hasta que se percató de la sustracción de fondos el día 23 siguiente. Discrepa también con el hecho no demostrado 9 de que se afirma no es ajeno al daño y al riesgo al que expuso al usuario de las cuentas. El recurrente identifica y explica las violaciones normativas en el apartado cuarto. Acusa así desatención a los mandatos 60 de la Ley Orgánica del Sistema Bancario Nacional y 613 del Código de Comercio, que le permiten establecer los términos y condiciones de sus contratos para obtener los beneficios de la banca electrónica,

pues se desconoció los deberes y obligaciones de las partes, en particular el del actor en cuidar el manejo de sus claves. Explica, el servicio BCR PERSONAS es un contrato adicional cuyo sustento es la relación contractual con el cuentacorrentista, pues el canal electrónico tiene efectos positivos o negativos en la cuenta corriente; el cliente libremente lo acepta, no tiene el deber de soportarlo, el uso de las claves es parte del acceso al servicio y el mecanismo de manifestación de voluntad del usuario. Reclama, desobediencia a los preceptos 702 y 704 del Código Civil, por cuanto no hay relación de causalidad entre el daño, ya que se determinó que los fondos se acreditaron en la cuenta de un tercero con una clave con la que sólo el actor cuenta y utilizada en México, según los registros informáticos; y no puede imponerse la indemnización pues no se demostró incumplimiento de alguna obligación contractual, el testigo perito indicó que sus sistemas son 100% seguros. Asevera, se vulneraron los artículos 35 de la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, no. 7472 (Ley del Consumidor), y el 1021 del Código Civil, en el tanto no se reconoció la relación contractual existente, con lo cual se está frente a responsabilidad contractual y no en responsabilidad objetiva, que es una modalidad de la responsabilidad extracontractual. Insiste, el acceso a las cuentas por Internet, sólo puede realizarse luego de suscribir un contrato, clave y contraseña habilitada por el cliente y encriptada. En este caso, enuncia, no es controvertido que el acceso se dio con la clave y contraseña del usuario. El uso y custodia de las clave es una obligación del cliente reconocida por el ordenamiento y la doctrina. Denuncia trasgresión a las reglas de la sana crítica cuando los juzgadores afirman que indujo a la parte actora a decir en la denuncia ante el OIJ que fue un hacker; restaron importancia al hecho de que cualquier usuario de Internet está expuesto a ser infiltrado. Cita doctrina en relación con el contrato bancario.

Explica, la responsabilidad contractual es subjetiva, relacionada con el dolo o la culpa, detrás de un incumplimiento de las condiciones de un contrato; la extracontractual, puede ser objetiva, se responde por la simple existencia del daño. Expresa, el mandato 35 de la Ley del Consumidor no implica que el comerciante deba responder siempre en forma inexcusable, pues le libera cuando hay ajenidad en el daño. Expone, las partes tienen entre sí una relación contractual, pero el canal de transmisión de datos en el servicio de Internet no lo hace éste, ni el cliente, lo brinda un tercer proveedor. Dice, elimina el riesgo de que terceros puedan acceder a su sistema, pero no al del cliente, a quien no le puede imponer conductas, limitando el acceso a sus fondos, ni verificar sus sistemas de información y el uso de su ordenador o los antivirus que posee. Esto es imposible y atenta contra los principios de razonabilidad y proporcionalidad. Sostiene, en el debate quedó claro que sus sistemas de información son seguros, de manera que implícitamente la falla en seguridad y diligencia fue del cliente. Las transacciones en su criterio fueron válidas, pues fue una orden de giro contra los fondos depositados en una cuenta, emanada por quien tiene las identificaciones respectivas. Menciona, el cliente asegura no entregó sus datos ni dio autorización, pero consta que digitó la totalidad de su clave dinámica y que los reveló. Prosigue, la responsabilidad es un tema general en Derecho, cita los cánones 41 y 46 de la Constitución Política, la normativa clásica se encuentra en el Código Civil, artículo 1045, que es la subjetiva, la que supone culpa; lo objetiva, sin culpa sólo existe por Ley expresa; la necesidad o no de culpa es lo que las distingue y la carga de la prueba, pero en ambas es indispensable la causalidad. Trascribe los mandatos 1045 y 1047 del Código Civil y doctrina. Reitera no da el servicio de Internet, sólo ofrece una ventanilla en Internet, el cliente es quien utiliza la red conforme a su proveedor de elección. Hace una analogía con los cajeros

automáticos, de manera que no se hace responsable por todo lo que ocurre en la calle por la que se accede al cajero. Observa, hay distinción entre lo que jurídicamente está obligado a hacer y lo que le conviene hacer. Si la falla no fue en su sistema, no hay nexo de causalidad. Arguye desobediencia al precepto 190 de la Ley General de la Administración Pública, ya que es evidente que hay un tercero, al que la parte actora divulgó su información cuando recibió el correo y que se impuso de esos datos, según señalan sus sistemas de información y registros, así como la testimonial pericial rendida. Recalca el Tribunal no discernió entre las medidas preventivas y de información a los clientes para que adquieran una conducta adecuada en el uso de la plataforma electrónica, y la violación de las medidas de seguridad que posee. Esgrime errónea aplicación del derecho a la información contemplado en el artículo 32 de la Ley del Consumidor, pues el fallo desconoce que informó al consumidor y advirtió de eventuales fraudes informáticos, pretirió la publicidad a la generalidad en la que se define que es “fishing” y se dan consejos. Refiere la sentencia 516-F-SI-2009 de esta Sala, de la que extrae que no hay responsabilidad por riesgo creado sin que se demuestre el funcionamiento anormal, que la culpa de la víctima por dar información a un tercero requiere comprobar el comportamiento privado del actor, lo que es ajeno a los bancos, que se deben aplicar las reglas de la sana crítica partiendo de la valoración de elementos probatorios que permitan desvirtuar la presunción de buena fe del actor. De esta manera, observa, con la demostración de que sus sistemas no fueron violados junto a la aplicación de la clave dinámica, es evidente que no hay función anormal del servicio y que el daño es posible que se derive de la imprudencia o falta de cuidado de la víctima en el manejo de su información. Añade, se infringe los cánones 193.b del CPCA y 222 del Código Procesal Civil, pues en su parecer había suficiente motivo para litigar, no actuó

de mala fe. Denuncia, falta de aplicación del mandato 5 del Reglamento de Tarjetas de Crédito no. 28712-MEIC, que establece como deber del tarjetahabiente usar personalmente su tarjeta, no mostrar las claves a cajeros y otros sistemas electrónicos y reportar al ente emisor el robo pérdida de la tarjeta, aplicable conforme a los artículos primero, 10 y 12 del Código Civil, ante la ausencia de un marco legal y regulatorio a la sistemas de información, a la materia de Internet Banking, donde la clave es personal, creada por el cliente, secreta, de su manejo exclusivo. El decreto mencionado contempla el deber de guardar las claves de acceso a los cajeros electrónicos o sistemas de información. Cita los preceptos 4, 8, 11, 14 y 23 del Reglamento de Servicios Electrónicos, que contemplan la responsabilidad del cliente de guardar sus claves de acceso. Disiente se le haya considerado esas normas abusivas o vejatorias, pues tienen sustento en la Ley del Consumidor. Por otra parte, esgrime desatención a los principios de razonabilidad y proporcionalidad. Puntualiza, en un régimen de libertad, no puede imponer a sus clientes conductas, tampoco verificar sus sistemas de información o el uso que hacen de sus ordenadores, ni los antivirus que posean. Menciona los mandatos 49 de la Carta Magna y 3 de la LGAP, por los cuales está sometido al principio de legalidad, y en este caso, con base en sus registros informativos, hubo voluntad de la parte actora de realizar las transacciones, y por ello no puede reconocer el reclamo que ella hace, pues de lo contrario "*habría un divorcio entre el motivo del actor*" según los artículos 132 y 133 de la LGAP. El artículo 35 de la Ley del Consumidor debe interpretarse y aplicarse en forma tal que no se genere un desequilibrio en la balanza o equilibrio de las prestaciones económicas que impera en toda contratación mercantil, deben los jueces valorar la equidad e las relaciones, no fracturarla o tornarla imposible. Manifiesta, la sentencia le impone garantizar al 100% la seguridad en el uso de Internet, lo que

es absurdo y atenta contra los principios constitucionales citados. Acota, los bancos dan servicios de información financiera, no brindan servicios de comunicación cibernética por estar vedado así en el canon 73 de la Ley no. 1644. Por último acusa infracción de los mandatos 132, 133 y 134 de la LGAP.

IV.- De la anterior reseña, se extrae que el recurrente plantea un reclamo por violación indirecta de las normas sustantivas 5 del Decreto 28712, 4, 8, 11, 14 y 23 del Reglamento de Servicios Eléctricos, 60 de la Ley Orgánica del Sistema Bancario Nacional, 613 del Código de Comercio, 1, 10, 12, 702, 704, 1021, 1045 y 1047 del Código Civil, 35 de la Ley del Consumidor, 190 de la LGAP, 41 y 46 de la Constitución Política, y a los principios de razonabilidad y proporcionalidad (A); así como un agravio (subsidiario) por inobservancia directa de los mandatos 193 del CPCA y 222 del CPC, en el tanto se le impusieron las costas (B).

V.- En lo que a la recriminación **A)** atañe, el Tribunal dispuso que el Banco estaba en la obligación de informar de manera oportuna y eficiente todos los alcances de las cuentas de ahorro y corriente y el manejo electrónico; la publicidad habría reforzado ese compromiso, pero no sustituye "*la aplicación mesurada y detallada de los diferentes elementos del compromiso de las partes*". Continuó, tampoco es suficiente el contrato y su lectura, pues se requiere que el cliente haya sido enterado a cabalidad de los verdaderos alcances, para que adoptase las previsiones necesarias y conociere los riesgos que asumía. Más adelante, puntualizó, la seguridad en los sistemas informáticos es una obligación de todo banco, y está dentro de los costos de operación, pero no elimina su responsabilidad en la sustracción de fondos. Aseguró, en cuanto al hecho de un tercero, la responsabilidad del canon 35 de la Ley del Consumidor es objetiva, y frente a esa persona el Banco asume las facultades de repetir lo pagado, pero no le

excluye el pago remitiendo la acción contra esa tercera persona, en especial cuando no está identificada y las posibilidades de recuperación se tornan inciertas. Respecto de la culpa de la víctima, expresó, si bien en la denuncia el señor Barrientos reconoció haber ingresado la totalidad de su clave dinámica, el sistema informático del Banco no fue violentado y la institución generó una campaña de publicidad orientando a sus clientes a no suministrar información de sus accesos electrónicos, en especial la totalidad de la clave dinámica, lo cierto es que "*no existe prueba alguna de que ese aspecto del contrato electrónico, sobre la imposibilidad que el sistema requiriera la totalidad de los datos de la clave dinámica, le fuera explicado a accionante. Recuérdese nuevamente, que no basta con la aceptación de las condiciones del contrato sino que este debe ser explicado a cabalidad, lo que se encuentra ayuno de elemento probatorio*". Precisó, "*respecto a* (sic) *las campañas de publicidad no se aporta prueba para demostrar el nivel de pauta publicitaria que se generó de ella, ni siquiera si fue utilizada, lo que en nada determina un aspecto negativo; todo sin perjuicio que la pauta publicitaria ayuda con los mecanismos de seguridad, pero no es eximente de responsabilidad por sí. Como ya se indicó en otras ocasiones, la oficina electrónica en esencia se equipara a una oficina física, de suerte que los riegos propios de la agencia física bancaria hasta el momento que el cliente se retira de esta son por cuenta de la institución bancaria, situación que ocurre semejante con respecto con las oficinas virtuales*". Agregó, la entidad "*pierde de vista el banco que él también debe proteger la información de sus clientes. De los datos aportados en expediente no se evidencia que fuera normal realizar transacciones por montos importantes, y menos desde IP ajena al país. Al respecto debe tener claro la entidad bancaria, que dentro de su servicio se encuentra obligado a manejar el perfil de su cliente, pues es sabido que existen*

mecanismos de control y fiscalización por parte de entidades gubernamentales para que las instituciones bancarias conozcan a su cliente, con esta información, la institución debe valorar si cumple o no los requisitos para abrir una cuenta bancaria, el origen de sus fondos, para lo cual debe realizar un estudio del perfil de cada uno de sus clientes, y tal información debe ser utilizada no solo en beneficio y protección del banco, sino en el servicio que brinda a sus usuarios. En el presente proceso los movimientos que se dieron en su cuenta no eran comunes, se trataba de direcciones IP foráneos en algunos casos, y además tratando de topar el máximo de transacciones electrónicas realizables en cada fecha en cada una de las cuentas, lo cual no ha sido desvirtuado por la entidad bancaria y más aún, tampoco el banco dentro del servicio que debe rendir ha implementado medidas de seguridad suficientes para exonerarlo de su responsabilidad". Prosiguió, "*Si en el plano material, lo único viable fuera la reducción del riesgo, de suerte que siempre existen márgenes de este, necesariamente correspondería al ente de consumo, asumirlos. Suma a lo antes dicho que el mismo testigo aportado por el Banco narró como para esas mismas fechas se conoció de la existencia de un intento de sustracción de información de los clientes, pero que no se adoptó una campaña de información para alertalos* (sic) *ante esa situación de peligro inminente que alguno saliera afectado. Lo que a nuestros ojos resulta un incumplimiento grave. Es claro para este órgano colegiado que el ente público ha adoptado mecanismos de protección, cada día más sofisticados y seguros, con inversiones de capital importante; más la parte débil de la relación sigue estando en el usuario quien no presenta ese tipo de beneficios. Consecuentemente es sobre esa línea donde deben adoptarse los mayores mecanismos de protección. Una y otra vez, debemos reiterar que el riesgo no puede suprimirse del todo, pero debe administrarse y reducirse en todo aquello que*

resulta previsible". Sobre el contrato virtual señaló no constaba que hubiese sido explicado, y las campañas de difusión, no se demostró "*como* (sic) *fueron pautadas*". Por todo lo anterior, concluyó, hubo una "*vulneración manifiesta al derecho a la información, lo que determina que resulte imposible darle efectos jurídicos a ese eximente de responsabilidad*". Destacó, el señor Barrientos no indicó que contestó un correo, sino que intentó ingresar a la página electrónica del Banco y allí se le solicitó la totalidad de los datos de acceso incluyendo la clave dinámica; el testigo perito manifestó que era imposible que utilizando la dirección exacta del banco se pueda llegar a cargar algún sistema que vulnere la seguridad, pero aceptó la existencia de virus y otros mecanismos engañosos que bien podrían haber hecho pensar al actor que estaba en la oficina virtual, cuando en realidad suministraba información a un tercero. No obstante, descartó, no hay culpa de la víctima pues se está "*en una situación de riesgo propio del servicio suministrado por el ente público y que es este quien debe asumirlo. Diferente es si se hubiera acreditado un descuido manifiesto o un acto mal intencionado del dueño de las cuentas, que hubiera negado la buena fe que debe existir en el cumplimiento de los contratos, lo que en este caso no se hizo.* (…) *es una interpretación de lo señalado por el actor en su denuncia ante el banco, texto por demás lacónico y que aporta poca información para poder tener por acreditado que esa persona ha incumplido parte de los deberes que en lógica le correspondían*". Estimó por último que los fallos citados por el Banco, en los cuales se ha negado responsabilidad de un banco en situaciones análogas cuando el usuario reconoce haber divulgado los mecanismos de seguridad, no son de aplicación al presente asunto, difieren sustancialmente ya que en aquellos, los individuos reconocieron que no debían brindar la

información y así lo hicieron, mientras que en éste se alegó precisamente la falta de información "*como base para el comportamiento del usuario final*".

VI.- Sobre la responsabilidad objetiva en la actividad bancaria. La actividad bancaria, en particular la custodia y administración de los fondos del público, está rodeada de una serie de mecanismos o servicios periféricos, que son ofrecidos a los clientes como un atractivo y se incorporan como facilidades anexas a la custodia y administración. Por sí misma, esa actividad genera un riesgo, que se puede ver acrecentado con el uso de esos instrumentos o servicios, tal es el caso de las tarjetas débito y crédito o del denominado Internet Banking o banca en línea. Este incremento en el riesgo está asociado o depende del servicio periférico particular de que se trate. Su manejo y disminución será proporcional a las medidas de seguridad que las entidades bancarias estén en posibilidad (jurídica) de vincular. En la dinámica de esta actividad, la entidad bancaria es el proveedor del servicio principal anotado (custodia y administración de los dineros), así como de los accesorios e instrumentos relacionados, como lo es la banca en línea o electrónica; el cliente, por su parte, asume entonces el carácter de consumidor. En esta relación, como se ha señalado en diversas oportunidades, resulta aplicable el régimen de responsabilidad objetiva que prevé el canon 35 de la Ley del Consumidor (en este sentido pueden consultarse las sentencias de esta Sala, no. 300-F-SI-2009, 778-F-SI-2012, 1568-F-SI-2012 y 1607-F-SI-2012). El sistema estatuido en esta norma, dispone en términos generales que los inconvenientes de una actividad lucrativa –como lo es la bancaria- sean asumidos por quien la despliega, con algunas precisiones. Y es que si bien se configura como una responsabilidad objetiva, al prescindir de la culpa y del dolo, la atribución no opera de pleno derecho o en forma automática. En este orden, además de la de acreditación de la conducta lesiva del agente, el esquema no está exento del

deber de demostrar la existencia de la lesión y el nexo de causalidad, y por tanto del criterio de imputación (riesgo). En cuanto al vínculo causal, admite el mismo numeral 35, la ruptura o eliminación en los casos en que el agente acredite ajenidad en el daño. Dicho de otro modo, cuando comprueba la existencia de al menos uno de los eximentes, cuales son el hecho de tercero y la culpa de la víctima. Por último, debe destacarse que en este particular régimen, el deber de reparar se construye o se funda en la existencia del daño, la conducta del agente en ejercicio de su actividad y el nexo de casualidad que existe entre estos dos elementos, al margen de que exista un convenio por escrito o no entre el consumidor y el agente.

VII.- En suma, tuvo por demostrado el Tribunal que en efecto los sistemas informáticos del Banco no fueron vulnerados para realizar las transacciones en cuestión, y que éste realizó una campaña televisiva, radial e impresa sobre la importancia de no entregar los datos de la clave dinámica; así lo detallan los hechos probados 20 y 6 de la sentencia recurrida y se reitera en los considerandos. También reconoció en el hecho 7, que el contrato que permite el ingreso al sistema de banca electrónica, establece la obligación de los clientes de no entregar los datos de la clave dinámica, y que esto debe ser aceptado para poder ingresar al sistema. Asimismo, determinó que al presentar el reclamo administrativo, el señor Barrientos indicó que al intentar revisar sus cuentas, notó que no podía ingresar, pues al ingresar su clave, el sistema le solicitó ingresar todos los números de su clave dinámica, los ingresó en dos ocasiones adicionales, sin que pudiese ingresar, y que en su denuncia ante el OIJ declaró que ingresó los datos para entrar a la página, pero dicha página era de un hacker (hechos 18 y 21). Pese a todo ello, determinó en lo medular (y como primer motivo), que el Banco de Costa Rica vulneró el derecho de información al señor Barrientos, en el tanto –en su parecer- no hay elementos que demuestren

se le hubiese explicado que la estipulación del contrato (y el "reglamento") en el sentido de que el sistema no le requeriría la totalidad de los datos de la clave dinámica. Esta Sala discrepa con esa determinación, con fundamento en las manifestaciones del testigo perito, señor Leihman Garita Rodríguez, quien describió en primer término, el proceso para obtener el servicio de banca en línea. Narró, el cliente tiene una cuenta de ahorro o corriente, solicita la tarjeta, la cual se entrega en un sobre lacrado que además contiene el pin, "*con esta información, la información de la tarjeta y el pin de la tarjeta, el cliente accede al servicio Banco BCR, a la página del Banco BCR, y entonces por medio de esta misma página, él se registra en la página para utilizar el servicio. ¿Cómo hace el registro el cliente de este servicio? Ok, necesita su número de cédula, necesita tener una tarjeta válida, de la cual el Banco le entregó físicamente con su pin, verdad, entonces el cliente digita el pin secreto que le entregó el Banco en sobre lacrado y la fecha de vencimiento de la tarjeta, la cual obviamente tiene que ser una fecha válida. Entonces el sistema se encarga de validar toda esa información, tanto es así que el número de cédula tiene que estar relacionado con la tarjeta* (…) *Adicionalmente a eso, el cliente tiene que digitar una clave para usar el servicio, de manera personalizada, esa clave la inventa él* (…) *mínimo ocho caracteres, que no sean palabras sencillas,* (…) *seguidamente el cliente tiene que haber leído y aceptado las condiciones del Reglamento de Banca Electrónica, porque sino, el servicio no se le va a dar. Ya con el cliente haber accesado* (sic)*, haberse afiliado al servicio, entonces adicionalmente a eso, si el cliente desea realizar transferencias electrónicas de sus cuentas hacia cuentas de un tercero, tiene que contar con la herramienta de seguridad que se llama clave dinámica. Entonces, el cliente tiene que apersonarse, físicamente a una oficina del Banco, identificarse y solicitar la tarjeta de clave dinámica. El Banco le entrega físicamente al*

cliente una tarjeta de clave dinámica, la cual igualmente viene en un sobre sellado y la tarjeta viene lacrada, es decir, viene con una pintura sobre los códigos que tiene la misma (sic)*. La cual el cliente tiene que agarrar una moneda o un dispositivo y quitarle la pintura para poder ver la información de la tarjeta. Con esa información de la clave dinámica, ya el cliente tiene su identidad, su usuario, su clave, que él mismo determinó y ya tiene su tarjeta de clave dinámica, entonces ya puede hacer uso del servicio. Adicionalmente a esto, cuando, antes de que el cliente pueda realizar una transferencia electrónica, tiene que matricular la tarjeta física que le dio el Banco de clave dinámica. ¿Cómo hace esto? Tiene que entrar al sitio de la página, el cual ya fue validada con su cédula y su clave, verdad, entonces, el sistema ya registró la tarjeta que el cliente, ¿por qué? Por que las tarjetas tienen, son 50 dígitos, tienen 50 coordenadas diferentes que tiene una tarjeta dentro de una matriz, la cual en buena teoría ninguna tiene que ser igual ni semejante. Entonces esta información, esta tarjeta el cliente tiene que activarla dentro del sitio, el cliente entra al sitio de la página del Banco BCR, accesa* (sic) *con su usuario y su clave válida, y entonces activa la tarjeta, para lo cual tiene que digitar tres coordenadas o un tripleta –como le decimos nosotros- una tripleta de datos que tiene la misma tarjeta que él tiene físicamente* (…) *Ya habiendo activado la tarjeta de clave dinámica, entonces ahora sí, ya tiene totalmente el uso y la administración de sus cuentas por medio de la herramienta de banco BCR*". Asimismo, señaló el señor Garita que desde el año 2007 hasta la fecha, la entidad ha mantenido en la página una leyenda o advertencia donde indica que nunca deben entregarse datos personales y que el Banco nunca le solicitará información personal por ningún medio, menos la información completa de su tarjeta de clave dinámica.

VIII.- Para esta Cámara, del procedimiento y requerimientos relatados por el testigo perito, se extrae que: 1) el cliente que habilita el servicio de banca electrónica tiene un conocimiento básico o bien de nivel medio para realizar ese procedimiento; 2) el contrato (si bien es de adhesión), es aceptado en su totalidad, incluyendo la obligación de no entregar los datos de la (eventual) clave dinámica; 3) es evidente para el usuario que la clave de usuario o de acceso es confidencial: es de su creación y tiene una serie de lineamientos que en caso de no cumplir no sería aceptada; 4) lo mismo ocurre con su tarjeta de clave dinámica. En cuanto a este dispositivo, es claro que el procedimiento determina que también contiene información para su uso personal, de su conocimiento exclusivo, nótese que debe presentarse a una oficina física del Banco, identificarse y allí recibe en un sobre sellado, dentro del cual se halla la tarjeta lacrada, luego debe proceder a habilitarla o matricularla. De esta forma, la estipulación contractual aceptada en forma primigenia por el señor Barrientos cuando habilitó para sí el servicio de banca en línea, encuentra además ejecución en todo el trámite descrito que hubo de realizar para ello y para realizar transferencias de fondos a terceros, en el cual se evidencia el carácter secreto o confidencial de la clave de acceso y de la tarjeta de clave dinámica y se manifiesta –como lógico- el correlativo deber de cuidado que ha de tener en el manejo de éstas. El Banco impuso todo este procedimiento para salvaguardar la confidencialidad de las claves, y es medianamente razonable que el cliente debió hacer lo propio por proteger ese estado.

IX.- A todos estos pasos y sus particularidades establecidos por la entidad y a los que se ajustó el señor Barrientos, se suman la advertencia que se halla en el sitio web del BCR desde el año 2007 y la campaña publicitaria. Recuérdese que el señor Barrientos se adhirió, se afilió al servicio el 13 de octubre de 2007 (hecho probado 5), de manera que en ese momento accedió a

la dirección o sitio web del Banco, bancobcr.com, la correcta u oficial. En ella se desplegaba la advertencia dicha y accedió al "*Reglamento para los Servicios de Banca Electrónica*". Aquel aviso se ha mantenido hasta la fecha, de manera que en todos los ingresos que hubiese hecho a la página de Internet del Banco, dicha información se desplegó. Valga insistir en que se acreditó que los sistemas de la institución no fueron vulnerados (distinto habría podido ocurrir en casos en que el usuario hubiese ingresado a páginas falsas con similitudes a la del Banco de Costa Rica, que no –necesariamente- consignan una leyenda en ese sentido; aunque llama la atención que, de conformidad con las manifestaciones del testigo perito, la página falsa a la que ingresó el señor Barrientos, mostraba ese aviso de que no debía ingresar todos los datos de la clave dinámica). A esto –como se adelantó- se añade la campaña televisiva, radial e impresa que desplegó el Banco en la línea de que los clientes no debían entregar la información de la clave dinámica (hecho probado 6). Así las cosas, de todo estos tres elementos que se extraen de la declaración del testigo perito, a saber, los procedimientos de afiliación y de transferencia de fondos a terceros, la advertencia en la página del Banco y la campaña publicitaria que desplegó, se concluye que don Emmanuel Barrientos sí había sido informado por la entidad bancaria de su obligación contractual de no entregar la información de su clave dinámica a ningún sujeto y que bajo ninguna circunstancia debía digitar todos sus datos.

X.- Por otra parte, no comparte esta Sala el reproche del Tribunal a la entidad bancaria por no advertir a sus clientes de la circulación de un virus en junio de 2011, por no adoptar mecanismos para la protección de la data de los clientes parte débil de la relación, ni instrumentos seguridad relacionados con el perfil de éstos, que le alertasen de los montos inusuales de las transacciones y desde direcciones IP foráneas. En primer término, se reitera que

para el año 2011, cuando ocurrieron las tres transacciones por las cuales se reclama responsabilidad, el Banco realizó una campaña publicitaria, que además contaba con advertencias y recomendaciones en su página, que el procedimiento para habilitar y utilizar el servicio de banca en línea, requería lectura y aceptación del "reglamento", y que había un trámite adicional necesario para efectuar transacciones a cuentas de terceros, con la matrícula y empleo de la clave dinámica, que era necesario solicitar y obtenerla físicamente en una oficina. Todo esto, a juicio de esta Cámara son medidas suficiente y razonables adoptadas por la entidad para la reducción del riesgo que implica el servicio de banca a través de Internet, son mecanismos de seguridad bastos que requieren un comportamiento del usuario que no excede el conocimiento básico que requiere cualquier sujeto para utilizar Internet ni el nivel medio para habilitar ese servicio y usarlo. De todas estas medidas se desprende lógicamente la confidencialidad de las claves y dispositivos y el deber del cliente de mantener ese estado.

XI.- Sobre estos temas, la prueba testimonial pericial indicó varios puntos que deben destacarse. Explicó el señor Garita Rodríguez, que las direcciones IP son un número único que identifica a una computadora, a nivel mundial, conectada a una red, varían en el tiempo y no pertenecen a una persona específica (en su mayoría); de manera que el Banco registra la IP desde la que el cliente se conecta, la valida porque es una dirección que existe. Cuando el abogado del demandado le cuestionó por qué si el sistema detecta que la dirección IP no es la original del cliente, sí acepta que la transacción es válida, a lo que respondió "(…) *porque ya se pasó por todo un proceso de seguridad, en este caso, como les indiqué ahora, el proceso por el cual el cliente se afilia al servicio, el cual tuvo que haberlo hecho con un dispositivo físico que fue tarjeta de débito o crédito, la clave o pin de la tarjeta* (…) *la información contenida en la tarjeta,*

que es la fecha de vencimiento, una clave que el digitó, el uso de la tarjeta de clave dinámica, entonces dentro de ese proceso de seguridad ya el cliente validó al usuario como tal, para que utilice el servicio, es decir, yo ya identifiqué que este es mi cliente (…), *entonces ¿por qué no se validan direcciones IP? Porque ¿qué sucede si un cliente en determinado momento cambia de dirección IP? Actualmente la infraestructura que tenemos a nivel general, a nivel por lo menos general de Costa Rica, se hacen modificaciones constantes de direcciones IP, porque entran nuevas empresas, salen empresas, se cambian nodos, estamos en un desarrollo tecnológico, entonces si llega un momento en que un cliente ya sea dentro de Costa Rica o hasta fuera de Costa Rica, necesita hacer un pago de un crédito, necesita hacer la compra de una propiedad o algo así por el estilo, y resulta que el Banco le dice que no puede realizar la transacción porque su dirección IP no es la habitual, muy probablemente, pues igualmente el cliente va a venir y le va reclamar al Banco que no pudo comprar la propiedad, o que el Banco le está cobrando una multa un pago de un crédito que no pudo realizar porque estaba en otra locación*". Sobre los elementos de seguridad de la página oficial del Banco, continuó interrogando el profesional "*El certificado como tal está encriptado pero ¿podría darse un link que se vaya a otra página X, que una persona común no sepa de qué se trata? ¿Se lo pregunto por su experiencia en la parte técnica?* [Testigo perito] *A raíz de la experiencia, hemos logrado observar que en la página falsa, por lo menos en este caso particular, era solamente una imagen, no tenía ningún link, por lo tanto si el cliente le daba click, no había nada*. [Abogado] *¿Y estéticamente la página era igual a la del Banco? ¿O no? En este caso*… [Testigo perito] *Estéticamente es semejante, si se notaron, si usted pone a comparación la página que estaba en el año 2011 contra la página del fraude, es muy semejante, no obstante, si se ve, si se ven campos muy abiertos, si se ve que la página es, si*

bien es cierto es semejante, pero no es igual. [Abogado] *¿Es posible que un hacker haga una página igual a la del Banco, y cuando yo cliente la acccese* (sic), *me direccione* (sic) *a una página falsa?* [Testigo perito] *si se refiere a que si yo al accesar* (sic) *la página original del Banco, me refiere hacia una página copia, verdad, hacia una página ilegal, no es posible, porque en ese caso hubiera tenido que vulnerar la seguridad de la página del Banco, y en este caso no se dio*. [Abogado] (…) *¿Y si se entra de un buscador?* [Testigo perito] *Si se entra de un buscador, los buscadores dependiendo de cómo usted haga la consulta, él le va a dar los resultados, eso ya queda directamente a decisión de la persona, porque si digamos yo entro a cualquier buscador, ya sea google, ya sea yahoo, y yo le pongo "Costa Rica", él me va a tirar un montón de links, de páginas donde se indique la palabra "Costa Rica", pero no necesariamente él va tirar cuál sea la página del Banco, verdad, la página oficial del Banco* (…) *por eso es que el Banco ha promocionado que se indique, y es parte de las recomendaciones de seguridad que el Banco siempre ha hecho, de que la persona no accese (sic) la página de la institución financiera Banco de Costa Rica, como de ninguna otra institución financiera, por medio de un buscador, sino que la digite manualmente como "www.bancobcr.com", eso está en las recomendaciones*. (…) [Abogado] *¿Puede ser que tire entonces un resultado de una página falsa?* [Testigo perito] *Podría hacerlo*. También le preguntó el licenciado Nassar si el Banco tenía conocimiento de que las IP de México eran utilizadas para actividades fraudulentas y sobre cuándo se dieron cuenta de eso, a lo cual respondió don Leihman que el Banco no estableció que la dirección IP es fraudulenta, no puede determinar si una dirección IP es esto. En este caso –apuntó- el Banco no plasmó que don Emmanuel recibió el correo, no obstante si determinó una relación de la dirección IP de México con el correo electrónico, pues este último trae una dirección IP que es

de donde es enviado, la cual se registraba en México, y por ello la relación del correo electrónico con el reclamo de don Emmanuel, pues las transacciones objetadas tenían esa dirección IP en México. Aclaró además, no hay herramientas para encontrar un IP fraudulenta, las herramientas son para seguridad del cliente, para que establezca seguridad perimetral para sus transacciones, ya que "*no necesariamente una dirección IP que se utilizó para un fraude, es una dirección que se utiliza siempre para un fraude*". Consultó el abogado "(…) *Si una IP se utilizó en algún momento para realizar alguna transacción fraudulenta, el Banco después puede validar esa misma IP para realizar otra transacción, ¿es viable en el Banco? ¿O no?* [Testigo perito] *El Banco registra la dirección IP desde la cual el cliente se conecta en el servicio bancobcr, la valida porque es una dirección IP que existe, en este caso, hay que recordar que las direcciones IP no son direcciones IP que pertenecen a una persona específica en su mayoría, entonces el hecho de que el Banco identifique como fraudulenta una dirección IP en* (sic) *base a una, dos o tres transacciones, sería como individualizar esa dirección IP, haciendo un juzgamiento anticipado, por que hay que recodar que el Banco la registra y la valida, pero no obstante antes de eso, establece todo un sistema de seguridad para acceso al servicio. Entonces, no obstante, si la dirección IP es solamente el medio por el cual se hace la transacción, pero no es la que valida los elementos de seguridad para, en este caso, para la institución, ¿Por qué? porque antes de eso yo ya validé que el cliente es quien dice ser por medio de lo que les indiqué ahora, una clave encriptada, una clave que sólo el cliente conoce y aparte de eso la información de la tarjeta de clave dinámica, la cual es solamente para el cliente, y la tripleta que se valida en relación con cada transacción*". Precisó, la dirección IP si puede indicar fraude, si hay un determinado número de clientes que indicasen ser objeto de fraudes desde una misma dirección, y se logre

establecer dentro del proceso de investigación que es la misma dirección IP. Más adelante, detalló que con anterioridad de los hechos que reclamó el señor Barrientos, la dirección IP no había sido utilizada en fraude, luego de la denuncia se utilizó en una o dos transferencias. Asimismo, sostuvo que cuando el Banco se percata de una página "*ilegal, que pueda tener información, que pueda poner en riesgo, no solamente a los clientes de la Institución, sino a clientes de otras Instituciones, solicita el cierre de la misma* (sic) *a las autoridades pertinentes*". Cuestionó el licenciado Nassar "*¿Farming es una copia de la página del Banco? O ¿me equivoco?* [Testigo perito] (…) *lo que hace es hacer una copia de una página de Internet de una institución financiera, o de cualquier otra institución, es hacer una copia de una página de Internet*. [Abogado] *Según su experiencia técnica y lo que usted nos ha indicado el día de hoy, ya que dejamos claro que no se sabe si llegó un correo o no al señor Barrientos, ¿pudo éste haber sido objeto de farming?* [Testigo perito] (…) *En* (sic) *base a la investigación realizada por mi compañera y mi persona, en base a lo que él mismo reclamante indicó en su nota de reclamo, se deduce que el señor Barrientos accesó* (sic) *a una página de farming, ¿por qué se deduce? Porque el Banco nunca solicita toda la información de la clave dinámica, tanto es así que en la página transaccional, perdón, en la página de entrada desde que el cliente ingresa al servicio ahí lo dice* (…) [Abogado] *Dentro de la declaración del señor Barrientos que usted nos leyó y que conoce, él dice que avisó al Banco la misma tarde que sucedieron los hechos, ¿Por qué el Banco no actuó congelando cualquier transacción en ese preciso momento?* [Testigo perito] *El Banco actúa de manera directa cuando el cliente dice que fue objeto de un fraude, de una estafa, como este caso, el Banco actúa directamente, ¿qué fue lo que sucedió en este caso en concreto? El dinero del señor Barrientos salió, fuera del Banco de Costa Rica, tanto fue así que las tres*

transferencias electrónicas fueron enviadas a una cuenta en el Banco San José, entonces, por medio de los protocolos que la oficina de investigaciones tiene, cuando la oficina de investigaciones es informada de que un cliente es alertado acerca de una posible estafa, entonces el Banco mueve el protocolo, para que la cuenta, en este caso, la cuenta destino, sea inmovilizada, a manera de prevención, porque también queda a criterio del Banco, en este caso del Banco San José si ellos inmovilizan la cuenta o no, verdad, pero el Banco si actúa. [Abogado] *¿El Banco de Costa Rica le indicó al Banco de San José esta situación?* [Testigo perito] *En el momento en que la oficina de investigaciones se percató de la situación, inmediatamente se procedió a hacer la notificación al Banco de San José, indicando que habíamos tenido esta situación, ¿qué es esta situación? Unas transferencias que viene un cliente que está reclamando, verdad, que fueron acreditadas en una cuenta del Banco de San José; entonces en este caso, gracias a ellos, pues si se inmovilizaron las cuentas donde se recibió el dinero, no obstante, en el momento en que ya se habían inmovilizado las cuentas, ya se habían hecho retiros de dinero.* De seguido la Jueza Loaiza inquirió al testigo perito. Así, preguntó "*¿Cuál es la razón que da el cliente para que él, de acuerdo con el formulario que usted tuvo acceso y nos leyó, ingrese todos los datos de clave dinámica? ¿Por qué lo hace el cliente?* [Testigo perito] *Esa es la consulta, porque digamos, vamos, esa misma consulta tendría yo, porque en la página del Banco, es más en esta página que yo les mostré que era una página falsa del Banco, que estaba circulando en ese entonces, en la misma página falsa indica dentro de las leyendas una advertencia que dice que no digite toda la información de su clave dinámica, no obstante el señor Barrientos sí lo hizo, él digitó toda la información de clave dinámica, entonces, ¿qué motivó a él a digitar toda la información de clave dinámica? Por eso es que hace una liga con el correo electrónico, porque*

el correo electrónico le dice señor cliente si usted no digita esa información sus cuentas van a ser cerradas, eso es lo que dice el correo electrónico de fishing que recibe el cliente, entonces aunando en lo que indica el cliente junto con toda la investigación que se hizo, se logra establecer un vínculo entre el correo de fishing y la acción que tomó el cliente de digitar toda su información, porque me imagino que en ese momento él no quería que le cerraran sus cuentas". El señor Leihman Garita señaló además que el cliente pudo haber creído estar en la página del Banco, pero lo que esa página le solicitaba era totalmente contrario a lo que el Banco le decía desde el año 2007, cual es que no digite la totalidad de su información de clave dinámica. Continuó la jueza Loaiza preguntado. "(…) *hay como* (...) *un banco de información, donde se registran las direcciones IP y que podemos determinar desde donde se hace la transacción; de la dirección IP que se usó aquí, nos dice usted que fue en México, ¿el Banco lleva algún listado de las direcciones IP en las cuales se han denunciado por parte de los clientes fraudes electrónicos? ¿Lleva un listado?* [Testigo perito] *El Banco mantiene un listado de las direcciones IP donde se ha generado fraudes antes.* [Jueza] *Esta dirección, concretamente en su investigación ¿pudo usted corroborar si había sido utilizada en otro fraude electrónico? La que se usó en esta.* [Testigo perito] *En ese momento dado, esa dirección IP, anterior a estos hechos, no había sido utilizada para realizar una estafa.* [Jueza] *¿Y posterior?* [Testigo perito] *Posteriormente a esa hubo una repetición en uno o dos casos, no obstante, igualmente fueron casos aislados.*" Prosiguió la juzgadora: "(…) *¿Era común que de las cuentas* (…) *se hicieran ese tipo de transacciones? ¿Tenía un perfil el cliente respecto de que era común que transfiriera millón doscientos, millón quinientos, un millón de colones? ¿Era común? ¿En su habitualidad de las negociaciones que realizaba? ¿Tenía perfil el cliente de si era común que el cliente transfiriera esos montos?*

[Testigo perito] *En este momento no podría precisarlo* (…) [Jueza] *¿Si en su investigación tomó este elemento en cuenta, si en su investigación pudo ver reflejado que las transferencias sobre estas cantidades eran comunes o no en las cuentas? O ¿no lo tomó en cuenta? O ¿no fue parte de su investigación?* [Testigo perito] *Si se toma en cuenta, pero en ese momento no lo pedí, no recuerda.* [Jueza] *Si hubiera sido pedido, ¿estaría plasmado en el informe que se realizó?* [Testigo perito] *No necesariamente, no obstante el informe yo no lo redacté, entonces eso lo hace el investigador de delito económico, yo soy investigador de delito informático, de la parte técnica, si el de delito económico consideró que valía la pena dejar en él, allí lo habría puesto.* [Jueza] *Dentro de los sistemas de seguridad del Banco, ¿el Banco tiene alertas para cuando, para cuando, de acuerdo al perfil del cliente, no acostumbra hacer transacciones elevadas de sus cuentas, aun cuando tenga la disponibilidad económica dentro de su cuenta? ¿Alerta? ¿Hay alguna alerta de seguridad que se dispara en el Banco* (…)*?* [Testigo Perito] *Para el servicio Banco bcr no, porque* (…) *se basa en otra estructura de seguridad diferente a la de nivel transaccional, porque hay personas que manejan mucho dinero, no necesariamente lo hacen en el mismo momento,* (…) *nosotros si hemos tenido casos donde la alerta se genera a nivel de ventanilla, cuando llega la persona y va a retirar un millón de colones y en su vida nunca había tenido un millón de colones en su cuenta, entonces el Banco si alerta sobre la salida del efectivo, el sistema sí nos alerta sobre la salida del efectivo, entonces el cajero no puede hacer la transacción hasta que nosotros validemos esa transacción, entonces esa alerta sí existe al nivel de caja, a nivel de plataforma; a nivel de medios electrónicos no existe dado que ya existe una validación previa de la transacción y tiene otros elementos de seguridad que en este caso no generan la alerta.* (…) *Hemos tenido casos donde una persona transfiere cierta cantidad de*

dinero, y después llega la otra persona en cuestión de cinco, diez minutos de haber recibido el dinero, a retirarlo, entonces nosotros paramos esa transacción; hemos tenido reclamos de clientes que llegan y nos objetan de porqué paramos esa transacción, a nivel de alerta, porque nos genera una alerta una persona que nunca había tenido (sic) *un millón de colones en su cuenta, y viene a retirarlo, que recibió por medio de una transferencia electrónica hace 20 minutos, entonces nosotros paramos esa transacción* (…) *el Banco se ha basado en reforzar las medidas de seguridad antes de la transacción*. [Jueza] (…)*¿Por qué no se ha implementado esa seguridad que tienen en los cajeros, en el sistema virtual? ¿No es viable electrónicamente? ¿Virtualmente no es viable?* [Testigo Perito] *Actualmente se está con un proyecto que abarca básicamente el manejo del perfil del cliente, no podemos decir que el banco puede medir cada transacción* (…) *entonces el Banco viene trabajado desde hace mucho tiempo, en herramientas que monitoreen esas transacciones, no obstante* (…) *el proceso para realizar una compra en una institución pública es bastante largo, y aparte de eso, son muchas transacciones* (…) *tendrían que revisarse a nivel diario, entonces, el Banco está trabajando en esa línea, no obstante ha hecho un reforzamiento de las herramientas de seguridad en el sitio, porque la prevención es mejor antes de que se realice el fraude a que durante que se realice el fraude* (…) *como ya existe un medio de seguridad, o varios medios de seguridad en la página, los cual el cliente siempre ha tenido conocimiento, los cuales son seguros, el Banco da cada transacción que se hace, en este caso por medio de banco BCR, como buena, es una transacción de buena fe, porque ya se validaron diferentes dispositivos de seguridad previo a realizar la transacción*. [Jueza] (…) *Hay alguna alerta en los sistemas de seguridad del Banco, respecto del perfil del cliente de que se está realizando transacciones desde una dirección IP fuera del país y, dentro de*

la habitualidad del cliente, no es costumbre utilizar esas direcciones IP? [Testigo perito] *Una alerta como tal no*. (…) [Jueza] (…) *Usted nos indicó que el actor pudo hacer recibido eventual un correo, respecto al fishing, un correo. El Banco teniendo conocimiento de la circulación de este correo, hizo comunicación expresa a cada uno de sus clientes sobre la alerta de este correo, de que estaba circulando por medios virtuales el correo?* (…) [Testigo perito] *A nivel masivo, así por medios de comunicación no, no obstante el Banco –como les indiqué ahora- siempre ha tenido un mensaje permanente con relación a que los clientes brinden su información personal o bien que reciban una llamada o un correo, o cualquier solicitud de información personal* (…) [Jueza] (…) *Masivamente no se especificó, ¿se mandó un correo a los clientes? ¿Si o no?* [Testigo perito] *En este caso concreto no.* (…) [Jueza] *De la investigación que ustedes realizan, ¿hacen un estudio del perfil del cliente?* [Testigo perito] Es parte de la investigación, sí. [Jueza] ¿*Qué elementos se toman en cuenta de esa investigación del perfil del cliente?* [Testigo perito] *inicia desde que se le solicita al cliente la denuncia judicial,* (…) *para establecer primero que todo, que el reclamo que él está planteando pues es verdadero, que no tiene tal vez alguna relación con autofraude, porque no es en este caso, pero sí en otros casos hemos tenido donde el cliente reclama una transferencia, pero resulta que la transferencia si era de él para él o para un tercero que él sí conoce, la investigación si determina eso. Entonces el Banco dentro del perfil de la investigación, si se revisa cómo es el cliente, dónde vive el cliente, si tiene alguna relación con la persona que recibió el dinero, si viven cerca, verdad, hace cuánto lo tenemos de cliente, si es un cliente nuestro, si es un buen cliente en aspectos económicos, me refiero, igualmente, desde hace cuánto tiene el servicio, desde hace cuánto tiene la cuenta, qué otros servicios tiene, qué otros servicios electrónicos, si tiene acceso a otros medios electrónicos como son las consultas*

electrónicas o transmisiones por teléfono, ese tipo de cuestiones se evalúan. [Jueza] *¿Y cuál es la finalidad de tener ese perfil? ¿De qué le sirve al Banco tener ese perfil?* [Testigo perito] (…) *la idea es tener conocimiento por parte, por lo menos en el caso del investigador, qué tipo de cliente es, cómo se maneja, en qué medios utiliza, ¿por qué? Porque en* (sic) *base a eso podríamos establecer cuál es el conocimiento o cuál pudo haber sido la causa o cuál es la experiencia que tiene el cliente con nuestros servicios.* (…)"

XII.- De lo anterior, en lo tocante a la falta de advertencia a los actores, y clientes en general, sobre el virus que circuló en junio de 2011, se observa que esa afirmación lo es respecto del correo electrónico que contenía un link o liga con una página falsa del sitio del Banco, según señaló el testigo perito. Éste informó que en la investigación se logró vincular aquel correo con una dirección IP en México y que las transacciones en cuestión se hicieron desde una IP en México, de ahí que se relacionó este correo con el caso del señor Barrientos. En primer lugar, se tiene que ese nexo no fue aceptado por el Tribunal, así se extrae del hecho no probado no. 1 y de su afirmación en el sentido de que el señor Barrientos nunca indicó haber recibido un correo. La existencia de ese correo para el Tribunal evidenció también la del "*virus*" o página falsa, de la que luego reprocha al Banco una falta de aviso concreta. Discrepa esta Sala, al margen de que el actor hubiese recibido un correo que le dirigiese a una página falsa, y de que habría sido conveniente el que hubiese recibido comunicación advirtiendo de ese correo y del virus, lo cierto es que el Banco tenía con el señor Barrientos un contrato que le imponía el resguardo de las claves y había hecho constantes esfuerzos publicitarios en el sentido de que no se le requería la totalidad de datos la clave dinámica, que ya en general advertían de situaciones y hechos como los del correo y el virus y página falsa. Por último, quedó claro también de lo manifestado

por el testigo perito que una vez identificado el cliente, con su número de cédula o usuario y su contraseña o clave de acceso, y autorizada la transferencia hacia un tercero con la tripleta de datos obtenida de la clave dinámica, el Banco tiene por válida la transacción, con independencia de la dirección IP desde la que se haya conectado el sujeto que posee y utilizó toda esta información. El establecimiento de la dirección IP es un elemento que se valora en la fase de investigación, pero explicó claramente el testigo perito, los clientes no siempre utilizan la misma dirección IP para conectarse. De esta manera se deduce que un mecanismo de seguridad que asigne una única dirección IP a los clientes no es viable en el estado actual del desarrollo de Internet. Tampoco lo es, según esa misma probanza, que se impidan transacciones por no ser direcciones IP usuales del cliente. La identificación y autorización dicha, se insiste la hace un sujeto que tiene todos los datos para ello, luego, más allá de los límites de cuantía que estableció el propio Banco (y que conocen sus clientes), no resulta razonable que deba denegar transacciones porque asciendan a montos que no acostumbra transferir el titular de las cuentas (y sus autorizados) a terceros.

XIII.- Por lo dicho hasta este punto, conviene señalar que en su demanda, Optomel y don Emmanuel Barrientos fundan sus pretensiones, primero en la falta de información (antes de la suscripción del servicio de banca electrónica y durante su prestación); segundo, en una (supuesta) vulneración a los sistemas informáticos del Banco, que determina incumplimiento de éste. Como se determinó en el considerando X, no existe en criterio de esta Sala violación al derecho a la información. En cuanto al alegado fallo del sistema del Banco, de su página en Internet, tuvo por demostrado el Tribunal (y se coincide) que no acaeció. Añade esta Sala, que en efecto, y contrario a las afirmaciones de la parte actora, el señor Barrientos no utilizó la

dirección y página del Banco de Costa Rica, sino a una página semejante, cuya intención era parecer la oficial del Banco y obtener todos los datos de clave de acceso y dinámica. Lo cual obtuvo. Adicionalmente, las transacciones fueron autorizadas con toda esa información. Luego, es razonable concluir, por la cronología de los demás hechos acreditados, que las transferencias las efectuó un sujeto o varios que se impusieron de aquella. Y ese conocimiento lo adquirieron por la actuación del señor Barrientos. En consecuencia, se configuró la culpa de la víctima, con lo que se rompe el nexo de causalidad entre la conducta del Banco (prestación del servicio) con el daño acusado. Por consiguiente, el agravio formulado deberá estimarse y el fallo se casará en estos términos.

XIV.- En mérito de lo expuesto, procederá declarar con lugar el recurso planteado. Se anulará la sentencia únicamente en cuanto denegó la excepción de culpa de la víctima y la falta de derecho, declaró con lugar parcialmente la demanda y ordenó al Banco de Costa Rica entregar y explicar a la parte actora los alcances concretos de los contratos y darle copia, reintegrar la suma de ¢3.700.000,00, los intereses, su indexación, y sufragar ambas costas del proceso. Fallando por el fondo, se acogerán las excepciones de falta de derecho y culpa la víctima. Así las cosas, la demanda ha de tenerse por desestimada en todos sus extremos. Como consecuencia de esto, se impone resolver sobre las costas del proceso, de las cuales se exonera a la parte actora vencida, de conformidad con el artículo 193.b del CPCA. Al respecto, encuentra esta Sala que la parte demandante tuvo suficiente motivo para litigar. Nótese que es luego del análisis de las probanzas aportadas y evacuadas, que se determina que el señor Barrientos ingresó a una página que intentó duplicar la del Banco, y no al sitio web oficial de la entidad, como creyó en todo momento y afirmó en su demanda. Es precisamente ese el fin que

persiguen las páginas que se catalogan como *farming*, hacer incurrir en error y obtener datos personales, sensibles y claves de la víctima, según lo explicó el testigo perito. Por consiguiente, es hasta la culminación de la etapa probatoria, de la comparecencia del señor Leihman, que la parte actora pudo empezar a asimilar lo acontecido, y que fue posible determinar finalmente que los hechos se enmarcan en la eximente de culpa de la víctima. Antes de ello, el señor Barrientos estaba en la convicción de que la falla había ocurrido en el sistema del Banco, así lo hizo ver en su escrito de demanda, tal es el grado de confusión que generó la página falsa. De esta manera, es clara la complejidad técnica del asunto, y en ello precisamente reside el que se acepte como eximente la convicción de la parte actora. En suma, ante la tecnicidad de las circunstancias fácticas, esta Sala considera que la parte demandante tuvo sufriente motivo para litigar.

POR TANTO

Se declara con lugar el recurso de casación planteado por el Banco de Costa Rica. Se anula la sentencia únicamente en cuanto denegó la excepción de culpa de la víctima y la falta de derecho. Fallando por el fondo, se acogen tales excepciones. Se resuelve sin condenatoria en costas.

Luis Guillermo Rivas Loáiciga

Román Solís Zelaya **Óscar Eduardo González Camacho**

Carmenmaría Escoto Fernández **Rocío Rojas Morales**

MACUNAQ