

**CONTRADICCIÓN DE TESIS 206/2020.
ENTRE LOS CRITERIOS SUSTENTADOS POR
EL PRIMER TRIBUNAL COLEGIADO EN
MATERIA CIVIL DEL DÉCIMO SEXTO CIRCUITO
Y EL DÉCIMO QUINTO TRIBUNAL COLEGIADO
EN MATERIA CIVIL DEL PRIMER CIRCUITO.**

**VISTO BUENO
SEÑOR MINISTRO
MINISTRO PONENTE: JORGE MARIO PARDO REBOLLEDO.
SECRETARIO: JORGE ARRIAGA CHAN TEMBLADOR.**

Ciudad de México. Acuerdo de la Primera Sala de la Suprema Corte de Justicia de la Nación, en sesión virtual correspondiente al día **diecisiete de marzo de dos mil veintiuno.**

**VISTOS; y,
RESULTANDO:**

PRIMERO. Denuncia de la Contradicción. Mediante Oficio número 2096/2020, remitido el nueve de octubre de dos mil veinte a través de la comunicación registrada con el folio ***** a la Oficina de Certificación Judicial y Correspondencia de la Suprema Corte de Justicia de la Nación, los Magistrados integrantes del Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito denunciaron la posible contradicción de tesis entre el criterio sostenido por el referido tribunal al resolver el juicio de amparo directo 176/2020 y el sustentado por el Primer Tribunal Colegiado en Materia Civil del Décimo Sexto Circuito al resolver el juicio de amparo directo 171/2018.

SEGUNDO. Trámite de la denuncia. Mediante acuerdo de quince de octubre de dos mil veinte, el Presidente de la Suprema Corte

CONTRADICCIÓN DE TESIS 206/2020

de Justicia de la Nación admitió a trámite la denuncia de la contradicción de tesis, ordenando formar y registrar el expediente bajo el número 206/2020.

Asimismo, solicitó a la Presidencia del Primer Tribunal Colegiado en Materia Civil del Décimo Sexto Circuito, remitiera versión digitalizada del original o, en su caso, copia certificada de la ejecutoria correspondiente, e informara si el criterio sustentado en ésta se encontraba vigente o la causa para tenerlo por superado o abandonado. En el mismo acuerdo se ordenó dar vista por conducto del MINTERSCJN a los Plenos en Materia Civil del Primer y Décimo Sexto Circuitos para su conocimiento respecto de la admisión de la presente contradicción de tesis.

Por último, se ordenó la remisión de los autos a la ponencia del señor Ministro Jorge Mario Pardo Rebolledo para la elaboración del proyecto de resolución.

TERCERO. Integración del asunto en la Primera Sala y avocamiento. Una vez recibidas las constancias requeridas al Primer Tribunal Colegiado en Materia Civil del Décimo Sexto Circuito por medio de las cuales informó que no ha abandonado su criterio, por acuerdo de cuatro de diciembre de dos mil veinte, dictado por el entonces Presidente de la Primera Sala de la Suprema Corte de Justicia de la Nación, se ordenó su integración al expediente y el avocamiento del asunto en la Primera Sala.

Al advertir que el asunto se encontraba debidamente integrado, se ordenó el envío de los autos a la ponencia del señor Ministro Jorge

Mario Pardo Rebolledo para la elaboración
del proyecto de resolución correspondiente.

C O N S I D E R A N D O:

PRIMERO. Competencia. Esta Primera Sala de la Suprema Corte de Justicia de la Nación es competente para conocer de la presente denuncia de contradicción de tesis de conformidad con los artículos 107, fracción XIII, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos; 226, fracción II, de la Ley de Amparo, vigente a partir del tres de abril de dos mil trece, y 21, fracción VIII, de la Ley Orgánica del Poder Judicial de la Federación, en relación con los puntos primero y tercero del Acuerdo General 5/2013, de trece de mayo de dos mil trece, del Tribunal Pleno de esta Suprema Corte, en atención a que el presente expediente versa sobre la denuncia de una posible contradicción de tesis suscitada entre criterios de Tribunales Colegiados de distinto Circuito, y el tema de fondo corresponde a la materia civil, en la que se encuentra especializada esta Sala.

Es aplicable, por las razones que informa, la tesis del Tribunal Pleno de esta Suprema Corte de Justicia de la Nación, de rubro: **“CONTRADICCIÓN DE TESIS ENTRE TRIBUNALES COLEGIADOS DE DIFERENTE CIRCUITO. CORRESPONDE CONOCER DE ELLAS A LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN (INTERPRETACIÓN DEL ARTÍCULO 107, FRACCIÓN XIII, PÁRRAFO SEGUNDO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, REFORMADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 6 DE JUNIO DE 2011)”**.¹

¹ Tesis P. I/2012 (10a.), Décima Época, publicada en la página nueve, del Libro VI, marzo de 2012, Tomo 1 del Semanario Judicial de la Federación y su Gaceta.

SEGUNDO. Legitimación. La denuncia de contradicción de tesis proviene de parte legitimada, de conformidad con lo previsto por los artículos 107, fracción XIII, segundo párrafo, de la Constitución Federal y 227, fracción II, de la Ley de Amparo, toda vez que fue realizada por los Magistrados integrantes del Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito.

TERCERO. Criterios de los tribunales contendientes. Las consideraciones contenidas en las ejecutorias pronunciadas por los órganos jurisdiccionales contendientes que dieron origen a la denuncia de contradicción son las siguientes:

I. Criterio del Primer Tribunal Colegiado en Materia Civil del Décimo Sexto Circuito, el cual sostiene la tesis aislada XVI.1o.C.3 C (10a.), de rubro y texto siguientes:

“TRANSFERENCIA DE FONDOS REALIZADA VÍA PORTAL DE INTERNET. CUANDO EL CUENTAHABIENTE NIEGA HABER DADO AUTORIZACIÓN AL BANCO PARA SU REALIZACIÓN Y ÉSTE AFIRMA HABER RECIBIDO LA INSTRUCCIÓN RELATIVA, CORRESPONDE AL PRIMERO DEMOSTRAR QUE EL SISTEMA QUE OPERA LAS FIRMAS ELECTRÓNICAS CARECE DE FIABILIDAD Y, POR TANTO, QUE SU CUENTA FUE SABOTEADA ELECTRÓNICAMENTE. *La transferencia electrónica es un instrumento de pago y de transacciones comerciales con cargo a la cuenta de un cuentahabiente, en la que es necesaria la intervención de uno o varios bancos, según se trate de una operación entre cuentas de una misma institución de banca múltiple o interbancaria, es decir, que los bancos actúan como expedidores, intermediarios o receptores de los fondos; sin embargo, para que los bancos actúen en esa cadena de relaciones, es indispensable que exista un iniciador de esa secuencia, o sea, un cuentahabiente ordenante y éste, para que pueda ingresar a su cuenta y girar instrucciones a la institución de crédito*

*sirviente, vía Portal de Internet, debe hacer uso de un dispositivo electrónico que le proporciona la propia institución, el cual, al accionarse, genera un número clave que, junto con las contraseñas y demás datos de identificación que el cliente crea confidencialmente, esto es, fuera del control del banco, deben introducirse al sistema operativo de cómputo a fin de que pueda llevarse a cabo la operación. **Por otro lado, la fiabilidad en la creación de la firma electrónica y de las distintas operaciones electrónicas que se realizan, vía Internet, otorgan certeza a la persona que la utiliza de que sólo ella la conoce, por lo que puede constituirle en una fuente válida y cierta de obligaciones;** además, las normas que versan sobre firmas electrónicas y operaciones que se ejecutan mediante la red de comunicación de que se habla, califican de válidos los actos jurídicos en los que se inserta una firma o se proporcionan claves de acceso y contraseñas, sin cuestionar la fiabilidad del método de uso, sino sólo el de su creación, de conformidad con los artículos 89 y 97 del Código de Comercio. En ese contexto, cuando el cuentahabiente niega haber dado su autorización al banco, para realizar la transferencia y la institución de crédito afirma que sí recibió la instrucción, **corresponde al primero demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad y, por tanto, que su cuenta fue sabotada electrónicamente, de conformidad con los artículos 1194 y 1195 del código citado.** Ello es así, **pues si bien es cierto que por regla general, es a las instituciones de crédito a quienes corresponde la carga de la prueba en tanto que cuentan con mayores elementos, como lo son los registros de las autorizaciones efectuadas por sus clientes, a que alude el numeral 57 de la Ley de Instituciones de Crédito, no menos lo es que el cuentahabiente bien puede exigir la aportación de esos registros y ofrecer, además, la prueba pericial en informática,** para acreditar que el banco se apartó de la forma de operar una transacción electrónica, o bien, que el sistema o método de creación de la firma electrónica no es fiable y, con ello, desvirtuar la presunción de que fue él quien con las claves de identificación, dio su autorización para que se llevara a cabo, con cargo a su cuenta, la transferencia de fondos que*

desconoce"².

La tesis aislada transcrita derivó de la resolución del juicio de **amparo directo 171/2018**, del cual se advierten los antecedentes y consideraciones siguientes:

- **Juicio oral mercantil.** ***** demandó en la vía oral mercantil a ***** el pago de \$*****, así como el pago del interés legal y los gastos y costas generados por el juicio interpuesto. Ello, con motivo del desconocimiento de una transferencia electrónica a la cuenta de un tercero registrada el veintidós de junio de dos mil quince.

Del juicio correspondió conocer al Juzgado de Oralidad Mercantil del Partido Judicial de León, Guanajuato, mismo que en sentencia de nueve de enero de dos mil dieciocho, condenó a la institución bancaria al pago de las prestaciones reclamadas, con excepción del pago de gastos y costas.

- **Juicio de amparo.** En contra de la resolución anterior, *****, promovió juicio de amparo directo del cual tocó conocer al Primer Tribunal Colegiado en Materia Civil del Décimo Sexto Circuito. Mismo que dictó sentencia el dieciocho de julio de dos mil dieciocho en el sentido de conceder el amparo.

Dicha determinación se sustentó, en lo que interesa para la resolución de la presente contradicción y por lo que se concedió el amparo, en los razonamientos siguientes:

- El órgano colegiado calificó como fundados los conceptos de violación en torno a que la autoridad responsable impuso al banco una indebida carga probatoria a fin de acreditar que el cliente realizó las transferencias de dinero de su cuenta a la cuenta de un tercero, vía portal de internet.
- Como punto de partida se señaló que la firma autógrafa es el medio por excelencia para crear el vínculo jurídico entre las partes que intervienen en la creación de un acto jurídico. Sin embargo, apuntó que los medios electrónicos han permitido la realización de operaciones comerciales entre personas no presentes.

² Consultable en la Gaceta del Semanario Judicial de la Federación, Libro 59, Octubre de 2018, Tomo III, página 2526.

- En cuanto a si la información que transmiten los datos electrónicos basta para constituir un acto jurídico dotado de validez, se dijo que ello había quedado resuelto por diferentes ordenamientos que establecen las reglas a las que debe ajustarse esta información para que se le reconozca valor jurídico.
- Por otra parte, señaló que la fiabilidad en la creación de la firma electrónica y de las distintas operaciones electrónicas que se realizan, otorga certeza a la persona que la utiliza de que sólo ella la conoce, por lo que puede constituirle una fuente válida y cierta de obligaciones.
- Así, que, una vez probado el método de creación de la firma electrónica, su ingreso al sistema de datos genera un vínculo jurídico que torna incuestionable la autoría del titular; y, en consecuencia, para desacreditarlo queda sólo la posibilidad de cuestionar la fiabilidad del método de su creación.
- Después, señaló que las normas respecto a las firmas electrónicas y operaciones que se ejecutan vía internet califican de válidos los actos jurídicos en los que se inserta una firma o se proporcionan claves de acceso y contraseñas, sin cuestionar la fiabilidad del método de uso, sino sólo el de su creación; de conformidad con lo dispuesto en los artículos 89 y 97 del Código de Comercio, mismos que se transcribieron. Asimismo, citó la tesis de tribunales colegiados de rubro siguiente: "FIRMA ELECTRÓNICA. REQUISITOS PARA CONSIDERARLA AVANZADA O FIABLE".
- Con base en lo anterior, afirmó que la institución bancaria, ante una acción sobre el desconocimiento de una transacción realizada vía portal de internet, sólo debe acreditar que se realizaron electrónicamente las operaciones que generaron los cargos por cualquier medio de prueba; por lo que será carga probatoria de quien niega la transacción el demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad o, en su caso, impugnar la certeza de la operación bancaria o comercial.
- Al respecto, abundó en cuanto a la distinción entre la fiabilidad de la firma electrónica y la certeza de la operación bancaria como fuente de obligaciones.

- Así, explicó que los elementos materiales de certeza en la operación bancaria, es decir, la seguridad de que quien realizó la operación es el titular de la cuenta, no encuentran sustento en el ámbito personal. Que éstos no están compuestos por la fecha y hora de la operación ni el análisis de su fiabilidad mediante la prueba pericial, sino que estos debían presumirse porque existe fiabilidad en su proceso de creación y en que los sistemas utilizados son estandarizados para realizar las operaciones comerciales mediante el uso de la firma electrónica.
- Por tanto, estimó que éste resulta fiable y constituía una fuente válida y cierta de obligaciones para los derechohabientes, cuando satisficiera los requisitos para su creación a menos que se demostrara que el proceso que le dio origen la hacía vulnerable.
- En otro aspecto, explicó que la transferencia electrónica es un instrumento de pago mediante el movimiento de fondos consistente en el cargo que recibe la cuenta del ordenante y el abono que se produce en la cuenta del beneficiario.
- Que, en la utilización de ese medio de pago, era necesaria la intervención de uno o varios bancos, según se tratara de una operación entre cuentas de una misma institución de banca múltiple o interbancaria, de tal suerte que los bancos actuarán como expedidores, intermediarios o receptores de los fondos, e incluso, con todas esas funciones a la vez, para el supuesto de trasposos entre cuentahabientes de una misma entidad bancaria. Empero, para que los bancos actúen en esa cadena de relaciones, señaló que era indispensable que existiera un iniciador de tal secuencia, es decir, un cuentahabiente ordenante, y un destinatario final que concluya el enlace de nexos, esto es, un cuentahabiente beneficiario.
- En atención a esa mecánica, expuso que resultaba necesario acreditar en caso de una transferencia cuyo importe no se acepta como cargo a la cuenta de la parte ordenante de la operación, que dicha operación fue realizada directamente por la institución de crédito, incumpliendo así su obligación de abstenerse de realizar retiros que sólo puede hacer la parte depositante.
- Apuntó que no debía perderse de vista que la transferencia de fondos se realizaba en forma electrónica, de tal suerte que era el sistema computacional del cliente el que se enlazaba con el sistema del banco, y en ambos sistemas informáticos quedaban registradas las operaciones de envío de la instrucción y recepción

de la misma, lo que permitía al cuentahabiente obtener un comprobante de la operación, pero también el sistema de la institución bancaria registrará de manera automática, como corresponde a los programas informáticos operados por computadoras, la autorización, asignándole un número, con fecha, monto, origen y destino.

- Lo anterior consideró que generaba que fuera el banco quien tuviere mayores elementos para acreditar no sólo la realización de las operaciones de transferencias electrónicas de fondos, sino también las autorizaciones correspondientes a cada una de ellas, ya que únicamente con base en la orden recibida por el sistema informático de la institución de crédito se puede realizar el traspaso automatizado de capitales.
- Por tanto, concluyó que como regla general la carga de la prueba sobre la existencia de la autorización para efectuar una transferencia electrónica de fondos correspondía a la institución bancaria. Sin embargo, que cuando el cuentahabiente afirmara que no fue él quien autorizó la operación y que por tanto la desconociere, pese a que es el único que pudo haber accedido a su cuenta, vía electrónica, utilizando el uso del dispositivo denominado “token”, y a través de las claves o contraseñas que integran la firma electrónica, mismas que dan acceso y la consecuente autorización a su sistema para realizar dicha operación, datos que ninguna persona, ni el propio banco conoce -a menos de que hubiese confiado a terceros esa información-; entonces correspondía al propio cuentahabiente demostrar que fue el banco quien se apartó de la forma de operar un pago a terceros, y en particular una transferencia electrónica, para lo cual podrá exigir no sólo la aportación de los registros del banco sino, inclusive, ofrecer la prueba pericial en informática, entre otros medios de comprobación a su alcance.
- El tribunal colegiado también consideró importante recalcar que las claves generadas por el uso del dispositivo denominado “token”, así como la de acceso y contraseñas, son datos que se crean bajo la confidencialidad del cuentahabiente; y que, por ende, se encuentran fuera del control de la institución de crédito. Entonces, que las operaciones bancarias y comerciales que se realizan a través de este medio electrónico, se presumen hechas por el titular de la cuenta o por la persona a quien se le hubiese confiado el uso del dispositivo y proporcionado las claves y contraseñas necesarias.

- En este sentido, se estimó que, si se actualizaba dicha situación, debía corresponder al cuentahabiente que desconoce un cargo hecho a su cuenta, desvirtuar la presunción de que se trata, y no a la institución de crédito.
- Asimismo, consideró que la institución bancaria, ante una acción sobre el desconocimiento de una transacción comercial realizada vía banca por internet, sólo debía acreditar, por cualquier medio de prueba, que se realizaron electrónicamente las operaciones que generaron los cargos -cuestión que no fue materia de debate-; por lo que sería carga probatoria de quien negara la transacción el demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad o, en su caso, impugnar la certeza de la operación bancaria.
- Con base en las premisas relatadas, determinó que, en la controversia sujeta a su consideración, al actor era quien debía probar que el sistema que operó su firma electrónica no fue confiable, o en su caso, que no fue él quien autorizó el cargo que se hizo a su cuenta bancaria, mediante el uso del dispositivo “token” y a través de las claves y contraseñas correspondientes, que sólo él debe conocer.
- Consecuentemente, consideró que debía presumirse que el cliente demandante fue quien realizó la transferencia o bien, que reveló la información necesaria para ello; por tanto, debía asumir las consecuencias de la falta de diligencia en el resguardo de los datos confidenciales que resultaban necesarios para que se pudiera realizar exitosamente la transferencia de recursos con cargo a su cuenta.
- Por todo lo anterior, el tribunal colegiado determinó que no estuvo en lo correcto la jueza responsable al sostener que era a la institución bancaria demandada a quien tocó probar que el cliente fue quien realizó la multicitada transferencia electrónica de dinero, vía portal de internet, utilizando el mecanismo “token” y a través de las contraseñas o datos de identificación necesarios para realizar exitosamente la operación, al declarar improcedentes las excepciones y defensas opuestas y, en consecuencia, condenar a la quejosa al pago de las prestaciones reclamadas.

Efectos de la concesión del amparo.

➤ En razón de lo anterior, el órgano colegiado concedió la protección constitucional para el efecto de que se dejara insubsistente la resolución reclamada, y se dictara otra en el que, siguiendo los lineamientos de la ejecutoria, normara correctamente las cargas probatorias y, con base en los medios de prueba ofrecidos y desahogados en el juicio resolviera lo que en derecho procediera.

II. Criterio del Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito, al resolver el juicio de amparo directo 176/2020, del cual se advierten los antecedentes y consideraciones siguientes:

- **Juicio oral mercantil.** Mediante demanda presentada el cinco de septiembre de dos mil diecinueve, ***** demandó ***** , la declaración judicial de inexistencia de diversas transferencias de dinero realizadas desde la cuenta que mantenía con dicha institución, y que sumaban la cantidad de \$***** , al no haberse realizado por la sociedad actora. Con motivo de lo anterior, se reclamó además el reembolso de dichas cantidades, el pago de los intereses legales sobre las citadas cantidades, así como el pago de gastos y costas que se generaran en el juicio.

Emplazada a juicio la institución demandada, ésta negó la acción de la actora aduciendo, fundamentalmente, que dichas operaciones se habían realizado con las contraseñas de la tarjeta de acceso, seguro y acceso digital y claves en posesión de la actora para realizar operaciones en internet.

Del juicio respectivo, conoció la Juez Sexto de lo Civil de Proceso Oral de la Ciudad de México, quien, seguido el juicio respectivo, dictó sentencia en el sentido de absolver a la parte demandada, sin hacer especial condena en costas para alguna de las partes. En contra de dicha resolución, la parte actora promovió juicio de amparo directo.

- **Juicio de amparo directo 176/2020.** Del juicio de amparo respectivo tocó conocer por razón de turno al Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito; mismo que concedió el amparo a la parte quejosa, en atención a los siguientes razonamientos:

- En primer lugar, precisó que el asunto puesto a su consideración se encontraba relacionado con la realización de cuatro transferencias a través de la banca electrónica que el actor no reconocía, por lo que solicitaba la devolución de los cargos realizados en su cuenta bancaria, así como los intereses legales generados.
- Detalló que, en la sentencia reclamada, la juez responsable determinó que la carga de la prueba de acreditar que las operaciones reclamadas no las realizó el cuentahabiente le correspondía a éste, pues, en su concepto, aquél debía demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad y, por tanto, que su cuenta había sido sabotada electrónicamente.
- En lo referente al estudio de fondo, se refirió al concepto de violación en que la parte quejosa adujo que la autoridad responsable había violentado lo establecido en el artículo 1194 del Código de Comercio al imponerle la obligación de acreditar un hecho negativo. A juicio de la sociedad actora, era la institución bancaria la que debía acreditar que ésta efectivamente había realizado toda y cada una de las transferencias electrónicas objeto de la controversia.
- Este argumento se calificó de fundado por el tribunal colegiado del conocimiento.
- Para motivar lo anterior, acudió a la forma en que el Código de Comercio regula las reglas relativas a la carga de la prueba, de acuerdo a lo previsto en sus numerales 1194, 1195 y 1196. De dichos preceptos, refirió que en los primeros artículos, la ley impone la carga de probar a quien cuenta con mayores facilidades para hacerlo, y que en el último de estos preceptos se establecía excepcionalmente la carga de la prueba a quien aduce una circunstancia opuesta a lo que comúnmente sucede.
- A partir de lo anterior, se refirió a la función de las instituciones bancarias como propietarios y administradores de los mecanismos a partir de los cuales se realizan las operaciones bancarias por medio de medios electrónicos. Señalando que dichas instituciones eran quienes tenían la obligación de establecer todo aquello que fuere seguro en su manejo e implementar los dispositivos y procedimientos que permitieran identificar las operaciones y los usuarios que se llevaran a cabo. Ello, a efecto de prevenir los actos ilícitos y su averiguación (sic).

- Apuntó que lo anterior significaba que tratándose de la demostración de actos efectuados mediante operaciones electrónicas, las instituciones bancarias tenían mayor facilidad de instrumentar los mecanismos necesarios para preconstituir la prueba de quienes ocurren a hacer operaciones en ellos, para aportarlas al procedimiento judicial en caso de suscitarse controversia, por ser quienes poseen los dispositivos, documentos, sistemas e instrumentos que emplearon para registrar la operación e identificar al usuario. Aunado a esto, consideró que incluso las leyes obligan a dichas instituciones a desplegar ciertas medidas de seguridad, están en aptitud de contar con sus resultados como medios de prueba.
- En cambio, consideró que el cliente encontraría gran dificultad frente al banco, porque no es el creador ni tiene a su alcance esos elementos operativos, de modo que le representaría una carga desproporcionada si se le exigiera presentarlos al juicio. Además, explicó que éste no tiene obligación ni generalmente aptitud para asimilar esos mecanismos, por corresponder a tecnologías del reporte de profesionales expertos y, en segundo, porque al ser la parte débil, es la que está sujeta a protección con las actividades de la parte fuerte, sin deber invertir las cosas.
- Sobre este punto, abundó en el deber de dar protección a los usuarios de los servicios bancarios, consagrado en los artículos 77 y 96 de la Ley de Instituciones de Crédito. Mismo que imponen a las instituciones bancarias la obligación de implementar todas las medidas de seguridad aptas para la protección de los valores manejados, de sus empleados, oficinas, usuarios, de los mecanismos e instrumentos utilizados, de conformidad con las disposiciones legales y administrativas aplicables, y con apego a las sanas prácticas que propicien la seguridad de esas operaciones y procuren la adecuada atención de los usuarios de tales servicios.
- Sobre este aspecto, acudió a las Disposiciones de carácter general aplicables a las instituciones de crédito, compiladas por la Comisión Nacional Bancaria y de Valores, publicadas en el Diario Oficial de la Federación el dos de diciembre de dos mil cinco. Así, luego de transcribir los numerales 314 y 316 del citado ordenamiento, el órgano colegiado se refirió particularmente al artículo 310 de las disposiciones generales referidas, el cual establece que las instituciones deberán utilizar factores de

autenticación para verificar la identidad de sus usuarios y la facultad de estos para realizar operaciones a través del servicio de banca electrónica.

- Posteriormente, conforme al artículo 316 bis 15 del mismo ordenamiento señaló que las instituciones deben generar registros, bitácoras, huellas de auditoría de las operaciones y servicios bancarios realizados a través de medios electrónicos y, en el caso de banca telefónica voz a voz, adicionalmente grabaciones de los procesos de contratación, activación, desactivación, modificación de condiciones y suspensión del uso del servicio de banca electrónica.
- De los preceptos anteriores, se extrajo que en la realización de las operaciones mediante el uso de elementos electrónicos, la institución bancaria tiene la obligación de asegurar que las operaciones estén consentidas por los usuarios, para lo cual es indispensable la presentación de por lo menos dos elementos de autenticación, así como el deber de conservar la información que justifique la realización de las operaciones y los medios por los cuales se autenticó el consentimiento del cliente.
- A partir de lo anterior, el tribunal colegiado concluyó que cuando se reclame la nulidad de las transferencias electrónicas, le corresponde a la institución bancaria soportar la carga probatoria de acreditar que las mismas se realizaron mediante el uso de los elementos de seguridad empleados para garantizar la fiabilidad de las operaciones y, además, que el sistema electrónico utilizado es fiable y que, por ende, no fue saboteado durante el lapso que se realizó la transferencia electrónica impugnada.
- Se dijo que la razón principal para optar por dicha peculiaridad en las reglas estrictas de la carga probatoria provenía de las circunstancias particulares en que se desarrollaba el caso de impugnación de transferencias electrónicas; siendo que en estas controversias, por regla general, el conocimiento técnico y las pruebas pertinentes para acreditar la fiabilidad del sistema electrónico y el empleo de las claves de seguridad, las detentan las instituciones bancarias. A partir de ello, se dijo que exigir de una forma irrestricta que fuera el cuentahabiente quien demostrara por sí solo ese elemento de la Litis, podría provocar lo que en doctrina se denomina con una carga probatoria diabólica, dado que se encuentra ciertamente limitado a obtener los medios de convicción idóneos.

- Los magistrados explicaron que la anterior consideración se justificaba de acuerdo a los principios de facilidad y proximidad probatoria, con base en los cuales debe satisfacer la carga de la prueba la parte que dispone de los medios de prueba y que puede producirlos o aportarlos al proceso a un menor costo para que pueda ser valorada por el juez.
- En efecto, refirieron que son las instituciones bancarias quienes pueden acceder con mayor facilidad a los medios de prueba para demostrar su actuar diligente y, además, acreditar la fiabilidad de sus sistemas. Por un lado, porque cuentan con personal especializado que goza de los conocimientos técnicos necesarios para determinar qué información puede ser relevante en el proceso y, por otro, porque con facilidad pueden acceder a diversos medios de prueba con mayor libertad que el cuentahabiente. Ello, dado que disponen y son propietarios-operadores de los sistemas por medio de los cuales se realizan las transferencias electrónicas.
- Por tanto, señalaron, si las pruebas relevantes se encuentran en muchas ocasiones en posesión o a disposición de las propias instituciones bancarias, o bien, éstas pueden acceder con mayor facilidad a la misma, entonces resulta inconcuso que a éstas les debe de corresponder la carga de la prueba.
- En razón de lo anterior, concluyeron que en atención a los principios de proximidad y facilidad probatoria debe exigírsele a las instituciones bancarias la carga de probar que su sistema electrónico es fiable y que, además, las transferencias de fondos se autorizaron mediante el empleo de los elementos de seguridad requeridos. Sin que a su juicio fuera correcto considerar que, cuando el cuentahabiente afirma que no fue él quien autorizó la operación y que por tanto la desconoce, toca a éste demostrar que fue el banco quien se apartó de la forma de operar un pago a tercero, y en particular una transferencia electrónica; ya que, se insiste, esa es una carga probatoria excesiva para el usuario del servicio bancario en función a que éste, de ordinario, no cuenta con acceso a los sistemas electrónicos de operación bancaria, ni tiene en su poder las bitácoras digitales que permitan demostrar la intrusión de un tercero ajeno al sistema.
- Se insistió que de imponer esa carga a los cuentahabientes sería transgredir los principios elementales de facilidad y proximidad probatoria, pues lo cierto era que la institución bancaria es la que

cuenta con la información y recursos tecnológicos necesarios para acreditar, en su caso, que la transferencia electrónica se autorizó mediante el empleo de elementos de seguridad y que, además, el sistema electrónico por medio del cual se realizaron es infalible, esto es, que no fue atacado o sabotado.

- Por su parte, en la ejecutoria se asentó que tampoco era dable sostener que las operaciones bancarias y comerciales realizadas a través de los medios electrónicos se podían presumir realizadas por el titular de la cuenta, pues lo cierto es que dichas operaciones se pudieron haber realizado mediante un sabotaje electrónico a la institución bancaria, ante la inobservancia de ésta a distintas disposiciones emitidas por la Comisión Nacional Bancaria y de Valores, por lo que en consecuencia, era a ésta a quien le correspondía acreditar no solamente que la transferencia electrónica se había realizado atendiendo a las Disposiciones Generales aplicables, sino que además se debía acreditar que el sistema electrónico utilizado para realizarlas era fiable y que, por tanto, no había sido vulnerado.
- En la misma tesitura, se hizo alusión a la situación ventajosa que guardan las instituciones financieras frente a los usuarios quienes son considerados la parte débil de la contratación y que, por tanto, requieren de protección especial a fin de compensar, en lo posible, tal desigualdad. Así, se afirmó que les corresponde a las entidades bancarias demostrar la legalidad de su actuación, y por tanto la demostración de los hechos controvertidos. Ello, toda vez que consideró que son dichas instituciones las que tienen mayor facilidad para aportar los medios de convicción que justifiquen su actuación, dado que cuenta con la información y todas las aptitudes técnicas para aportar los elementos de prueba necesarios para dirimir los conflictos suscitados con un cuentahabiente, lo que no ocurre con el usuario del servicio, quien consideró que encuentra serias limitaciones para justificar que no llevó a cabo la operación objeto de la controversia o que esta última fue realizada sin su consentimiento.
- Otra de las razones que otorgó el tribunal colegiado para sustentar que la carga de la prueba correspondía a la institución de crédito demandada y no al actor, consistió en que, en la actualidad, existe una tendencia uniforme en considerar a los mecanismos empleados por los bancos como factor generador de riesgo para las masas de usuarios; cuestión que, a la postre, lleva a la tutela de los consumidores a través de una modalidad de responsabilidad, de la que sólo se podrían liberar los proveedores

con la prueba de que tomaron todas las medidas para el funcionamiento óptimo de los servicios que prestan, fortalecidas con el empleo de los mecanismos más seguros y eficaces creados por la ciencia y la tecnología que ofrezca el mercado.

- Sobre este punto se precisó que una razón adicional para considerar que la carga de la prueba corresponde a la institución de crédito demandada, consistente en los principios rectores del derecho del consumidor, la indiscutible profesionalización y la alta especialidad de los bancos que impone la obligación de brindar la más amplia seguridad a los usuarios, mediante el empleo y actualización de los mecanismos tecnológicos y científicos más avanzados y menos vulnerables a los riesgos de interferencia por personas ajenas, de modo que las facilidades existentes para interferir en sus sistemas genera una presunción de culpa indirecta del prestador del servicio.
- A mayor abundamiento, se estimó que el criterio desarrollado resultaba congruente con la doctrina constitucional que se ha empezado a desarrollar por el Alto Tribunal en relación con la carga de la prueba tratándose de controversias mercantiles donde se disputen acciones derivadas de la prestación de servicios bancarios.
- Particularmente, se hizo alusión a la contradicción de tesis 128/2018, resuelta por la Primera Sala de la Suprema Corte de Justicia de la Nación en que el punto de contradicción radicó en determinar a quién le correspondía la carga de la prueba cuando en un juicio mercantil se ejercía la acción de nulidad de vouchers emitidos por la realización de una operación comercial efectuada con una tarjeta bancaria, y el consentimiento de la persona se había emitido mediante un número de identificación personal (NIP).
- Después de referirse a las particularidades del criterio referido, el tribunal colegiado estimó que resultaba viable considerar que, por analogía, algunas de esas consideraciones también resultaban aplicables en las controversias mercantiles en las que se demandara la nulidad de alguna transferencia electrónica.
- Para considerar lo anterior, se estableció que la propia Primera Sala del Alto Tribunal en el criterio referido dio cuenta de los distintos y complejos métodos empleados por los delincuentes cibernéticos para vulnerar y violar los sistemas electrónicos

utilizados por las instituciones bancarias para la ejecución de actos de comercio por lo que, a juicio del tribunal colegiado, no existía razón jurídica fundada para pensar que esos métodos, o incluso otros más complejos, no eran empleados por la población delictiva para obtener un provecho económico indebido, también, por medio de transferencias electrónicos pues, lo cierto, es que el avanzado contexto científico y tecnológico permiten a los delincuentes estar, muchas veces, un paso delante de los medios de seguridad adoptados por las instituciones bancarias.

- Al tenor de lo anterior, a juicio de los magistrados resultaba plena y abiertamente ilegal atribuirle prima facie la carga de la prueba a los usuarios de servicios financieros pues consideraron que estos encuentran un altísimo grado de dificultad para acreditar la vulneración a un sistema electrónico que les es del todo ajeno pues, se reitera, el sistema bancario es sumamente complejo, técnico y profesionalizado.
- En tal orden de ideas, en la ejecutoria se insistió que atribuirle esa carga de la prueba al actor, además de ilegal, era desproporcionado debido a que, en la mayoría de los casos, ello se erigiría como una carga diabólica de la prueba, en función a que lo ordinario es que los particulares se encuentren impedidos materialmente para allegar pruebas idóneas y directas que pongan de manifiesto la inseguridad de los sistemas informáticos utilizados por el banco.
- No obstante, se reconoció que dicha carga de la prueba podía ser atribuida al accionante cuando el banco demandado acreditara plenamente que no había ocurrido una vulneración a los sistemas durante la realización de la transferencia y que además había tomada las medidas de seguridad necesarias para la fiabilidad de la operación. En dicho supuesto, se apuntó que la carga de la prueba se revertiría al usuario quien tendría que desvirtuar las pruebas y actuaciones aportadas por la demandada.
- Apuntado lo anterior, se estableció que en el caso concreto, la negativa de la actora de haber realizado las transferencias electrónicas, objeto de la controversia, no encerraba ninguna afirmación, de modo que en términos del artículo 1195 del Código de Comercio, el actor no se encontraba obligado a probarla.
- En cambio, se estableció que el banco había afirmado que las operaciones bancarias se habían realizado en cumplimiento de todas y cada una de las disposiciones necesarias y al efecto la

demandada había expresado que se habían seguido todos los pasos de seguridad establecidos por los ordenamientos jurídicos que regulaban tal actividad. Aspecto que a juicio del Tribunal Colegiado correspondía demostrar a la institución bancaria con fundamento en el artículo 1194 del Código de Comercio, por ser la base en la que se sustentaba su posición.

- De esta manera, se precisó que si en el caso la institución de crédito había afirmado que para la autorización de las transferencias electrónicas se habían seguido todos los pasos de seguridad establecidos por los ordenamientos jurídicos, le correspondía probar que la actora efectivamente realizó la citada transferencia siguiendo el procedimiento y conforme al protocolo de seguridad establecido.
- Así, se concluyó que, contrario a lo sostenido por la autoridad responsable, la carga de probar que las operaciones impugnadas fueron realizadas por la actora asistía a la institución bancaria y no así a la quejosa, pues era la primera la que había realizado diversas afirmaciones, lo que le imponía la carga de probarlas; aunado a que conforme a la referida normatividad, contaba con mayor facilidad para probar sus afirmaciones.

Efectos de la concesión del amparo.

- A partir de las consideraciones antes desarrolladas, el Tribunal Colegiado concedió el amparo a la parte quejosa para el efecto de que la autoridad responsable dejara insubsistente el acto reclamado, y en su lugar dictara uno en el que determinara que la carga probatoria de acreditar que las transferencias electrónicas controvertidas fueron realizada por la actora, correspondía a la institución bancaria demandada.

CUARTO. Existencia de la contradicción de tesis. Sentada la reseña de las ejecutorias materia de análisis, debe determinarse a continuación si existe la contradicción de tesis denunciada.

Para resolver sobre la existencia de la contradicción de tesis que denuncian los Magistrados integrantes del Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito al resolver el juicio de

amparo directo 176/2020, debe analizarse si los órganos contendientes que son materia de la denuncia, sostuvieron tesis contradictorias, entendiéndose por tesis, el criterio adoptado por el juzgador a través de argumentaciones lógico jurídicas para justificar su decisión en una controversia. Ello, en tanto que lo que determina la existencia de una contradicción, es que dos o más órganos jurisdiccionales terminales del mismo rango, adopten *criterios jurídicos discrepantes sobre un mismo punto de derecho*, o sobre un problema jurídico central, independientemente de que las cuestiones fácticas que rodean los casos que generan esos criterios no sean iguales, ya que las particularidades de cada caso no siempre resultan relevantes, y pueden ser sólo adyacentes.

Así, la finalidad que persigue la resolución de una contradicción de tesis denunciada ante la Suprema Corte de Justicia de la Nación, está contenida en los artículos 107, fracción XIII, constitucional y 225 a 227 de la Ley de Amparo vigente; de los cuales se desprende una facultad para unificar los criterios interpretativos que dos o más tribunales colegiados -o las Salas de la Corte, en su caso- llegaren a adoptar a la hora de resolver algún conflicto; lo que proporciona certidumbre en las decisiones judiciales y otorga mayor eficacia a su función unificadora de la interpretación del orden jurídico nacional.

Derivado de lo anterior es posible afirmar que, para la procedencia de una contradicción de tesis, deben verificarse las siguientes condiciones:

1. Que los tribunales contendientes hayan resuelto alguna cuestión litigiosa en la que se vieron en la necesidad de ejercer el arbitrio

judicial, a través de un ejercicio interpretativo mediante la adopción de algún canon o método, cualquiera que fuese.

2. Que entre los ejercicios interpretativos respectivos exista al menos un tramo de razonamiento en el que la diferente interpretación ejercida gire en torno a un mismo tipo de problema jurídico: ya sea el sentido gramatical de una norma, el alcance de un principio, la finalidad de una determinada institución o cualquier otra cuestión jurídica en general; y
3. Que lo anterior pueda dar lugar a la formulación de una pregunta genuina acerca de si la forma de acometer la cuestión jurídica es preferente con relación a cualquier otra que, como la primera, también sea legalmente posible.

Lo que se busca es detectar un diferendo de criterios interpretativos más allá de las particularidades de cada caso concreto, como lo ha determinado el Pleno de este Alto Tribunal en la tesis jurisprudencial P.J. 72/2010, de rubro: ***“CONTRADICCIÓN DE TESIS. EXISTE CUANDO LAS SALAS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN O LOS TRIBUNALES COLEGIADOS DE CIRCUITO ADOPTAN EN SUS SENTENCIAS CRITERIOS JURÍDICOS DISCREPANTES SOBRE UN MISMO PUNTO DE DERECHO, INDEPENDIENTEMENTE DE QUE LAS CUESTIONES FÁCTICAS QUE LO RODEAN NO SEAN EXACTAMENTE IGUALES.”***³.

³ Tesis: P./J. 72/2010, Jurisprudencia, Novena Época, Pleno, Semanario Judicial de la Federación y su Gaceta XXXII, Agosto de 2010, Página: 7, Registro: 164,120, cuyo texto es del tenor siguiente: “De los artículos 107, fracción XIII, de la Constitución Política de los Estados Unidos Mexicanos, 197 y 197-A de la Ley de Amparo, se advierte que la existencia de la contradicción de criterios está condicionada a que las Salas de la Suprema Corte de Justicia de la Nación o los Tribunales Colegiados de Circuito en las sentencias que

Con base en lo anterior, esta Primera Sala debe verificar si se cumplen los requisitos para la existencia de una contradicción de tesis.

A juicio de esta Primera Sala, en el caso se actualizan el primer y segundo requisito para la existencia de la contradicción. En relación con el caso en concreto, conviene referir a que, si bien la argumentación a la que acudieron los tribunales colegiados de circuito contendientes para llegar a las conclusiones opuestas fue diversa, esta Primera Sala advierte que los órganos en discordia se enfrentaron a la misma cuestión jurídica.

pronuncien sostengan ‘tesis contradictorias’, entendiéndose por ‘tesis’ el criterio adoptado por el juzgador a través de argumentaciones lógico-jurídicas para justificar su decisión en una controversia, lo que determina que la contradicción de tesis se actualiza cuando dos o más órganos jurisdiccionales terminales adoptan criterios jurídicos discrepantes sobre un mismo punto de derecho, independientemente de que las cuestiones fácticas que lo rodean no sean exactamente iguales, pues la práctica judicial demuestra la dificultad de que existan dos o más asuntos idénticos, tanto en los problemas de derecho como en los de hecho, de ahí que considerar que la contradicción se actualiza únicamente cuando los asuntos son exactamente iguales constituye un criterio rigorista que impide resolver la discrepancia de criterios jurídicos, lo que conlleva a que el esfuerzo judicial se centre en detectar las diferencias entre los asuntos y no en solucionar la discrepancia. Además, las cuestiones fácticas que en ocasiones rodean el problema jurídico respecto del cual se sostienen criterios opuestos y, consecuentemente, se denuncian como contradictorios, generalmente son cuestiones secundarias o accidentales y, por tanto, no inciden en la naturaleza de los problemas jurídicos resueltos. Es por ello que este Alto Tribunal interrumpió la jurisprudencia P./J. 26/2001 de rubro: ‘*CONTRADICCIÓN DE TESIS DE TRIBUNALES COLEGIADOS DE CIRCUITO. REQUISITOS PARA SU EXISTENCIA*’, al resolver la contradicción de tesis 36/2007-PL, pues al establecer que la contradicción se actualiza siempre que ‘al resolver los negocios jurídicos se examinen cuestiones jurídicas esencialmente iguales y se adopten posiciones o criterios jurídicos discrepantes’ se impedía el estudio del tema jurídico materia de la contradicción con base en ‘diferencias’ fácticas que desde el punto de vista estrictamente jurídico no deberían obstaculizar el análisis de fondo de la contradicción planteada, lo que es contrario a la lógica del sistema de jurisprudencia establecido en la Ley de Amparo, pues al sujetarse su existencia al cumplimiento del indicado requisito disminuye el número de contradicciones que se resuelven en detrimento de la seguridad jurídica que debe salvaguardarse ante criterios jurídicos claramente opuestos. De lo anterior se sigue que la existencia de una contradicción de tesis deriva de la discrepancia de criterios jurídicos, es decir, de la oposición en la solución de temas jurídicos que se extraen de asuntos que pueden válidamente ser diferentes en sus cuestiones fácticas, lo cual es congruente con la finalidad establecida tanto en la Constitución General de la República como en la Ley de Amparo para las contradicciones de tesis, pues permite que cumplan el propósito para el que fueron creadas y que no se desvirtúe buscando las diferencias de detalle que impiden su resolución.”.

Al respecto, se advierte que ambos órganos colegiados ejercieron su arbitrio judicial al conocer de una controversia en la que una institución bancaria fue demandada en la vía oral mercantil, con motivo de que la persona con la que tenía celebrado una relación contractual desconociera determinadas transferencias de dinero, realizadas por medio de la banca por internet.

En ese sentido, como se advierte de la síntesis de los criterios realizada en el considerando anterior, se tiene que en los juicios de amparo directo que tenían a su consideración, ambos tribunales debían definir la parte a quien debía corresponder la carga probatoria de acreditar la validez de las transferencias electrónicas, particularmente, que no se hubieren violentado los elementos de seguridad dispuestos por la institución bancaria a efecto de asegurar la fiabilidad de las transacciones realizadas de manera electrónica.

Cabe precisar que, en ambos supuestos, las resoluciones objeto del acto reclamado, se refirieron a la correspondencia de la carga probatoria, con fundamento en lo dispuesto en los artículos 1194, 1195 y 1196 del Código de Comercio, así como en la normativa especial referente a las instituciones de crédito; siendo que arribaron a posturas disímiles entre sí.

Así, se advierte que, por un lado, el Primer Tribunal Colegiado en Materia Civil del Décimo Sexto Circuito sostiene que “(...) cuando *el cuentahabiente* niega haber dado su autorización al banco, para realizar la transferencia y la institución de crédito afirma que sí recibió la instrucción, corresponde al primero demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad y, por tanto, que su cuenta fue sabotada electrónicamente (...)”.

En contraposición a lo anterior, el Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito, al resolver el juicio de amparo directo 176/2020, determinó que *“(…) cuando se reclame la nulidad de transferencias electrónicas, le corresponde a la institución bancaria soportar la carga probatoria de acreditar que las mismas se realizaron mediante el uso de los elementos de seguridad empleados para garantizar la fiabilidad de las operaciones y, además, que el sistema electrónico es fiable y que, por ende, no fue saboteado durante el lapso en que se realizó la transferencia electrónica impugnada.”*⁴.

De las consideraciones expuestas, esta Primera Sala llega a la conclusión que los criterios resultan efectivamente disímiles en relación con el mismo punto de derecho. Lo anterior, se considera así, en tanto ambos órganos llegaron a conclusiones opuestas respecto de cuál de las partes en juicio debía demostrar la fiabilidad del sistema electrónico por medio del cual se hubiere realizado una operación bancaria cuya validez resultara controvertida.

No obsta a lo anterior, que, al resolver el juicio de amparo directo 176/2020, el Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito hubiere hecho referencia al criterio sostenido por esta Primera Sala al resolver la contradicción de tesis 128/2018, del que derivó el criterio de Jurisprudencia 1a./J. 16/2019 (10a.), de rubro: “NULIDAD DE PAGARÉ (VOUCHER). CARGA DE LA PRUEBA DE LAS OPERACIONES EFECTUADAS MEDIANTE EL USO DE TARJETA BANCARIA AUTORIZADAS A TRAVÉS DE LA DIGITACIÓN

⁴ Sentencia dictada el diecinueve de agosto de dos mil veinte en el juicio de amparo directo D.C. 176/2020 por el Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito, página 19, párrafo 44.

DEL NÚMERO DE IDENTIFICACIÓN
PERSONAL (NIP) EN DISPOSITIVOS
DENOMINADOS "TERMINAL PUNTO DE
VENTA".

Ello, en virtud de que el objeto al que se refiere el criterio citado, si bien guarda similitud con la problemática que ahora se suscita, no resulta el mismo punto jurídico al que correspondió pronunciarse a esta Primera Sala en aquella oportunidad. Esto es, mientras que en la contradicción de tesis referida este Alto Tribunal estableció que la institución se encuentra obligada a ofrecer las pruebas pertinentes que acrediten que fue el propio usuario quien digitó su número de identificación personal, ante la demanda de nulidad de los vouchers emitidos con motivo del uso de una determinada tarjeta bancaria mediante la autenticación a través del mecanismo denominado CHIP y NIP; en el caso que tuvo a su consideración el Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito procedió determinar a quién correspondía acreditar la vulneración en los sistemas de seguridad, ante la demanda de nulidad de una transferencia de dinero utilizando los medios electrónicos y digitales provistos por la institución bancaria.

De esta manera, se estima que el objeto de pronunciamiento no resultaba idéntico al adoptado por esta Primera Sala y que, por tanto, las consideraciones emitidas por el citado tribunal colegiado, no constituyen una mera reiteración de las consideraciones contenidas en la Jurisprudencia 1a./J. 16/2019 (10a.). En cambio, se advierte que el Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito, al resolver el juicio de amparo directo 176/2020, desarrolló consideraciones adicionales tendientes a justificar la adopción de la misma conclusión lógica, dentro de lo que destacan consideraciones

respecto a la protección de los usuarios del servicio financiero en su calidad de consumidores, así como la cita de diversos preceptos de las Disposiciones de carácter general aplicables a las instituciones de crédito, emitidas por la Comisión Nacional Bancaria y de Valores, y publicadas en el Diario Oficial de la Federación el dos de diciembre de dos mil cinco.

Finalmente, se cumple el tercer y último requisito de existencia de la contradicción de criterios que nos ocupa, para lo cual se estima que corresponde a esta Primera Sala definir si debe ser el cuentahabiente o a la institución bancaria quien deba probar la fiabilidad de los mecanismos de banca electrónica cuando en un juicio se reclame la nulidad de una transferencia de dinero utilizando dicho mecanismo.

QUINTO. Estudio de fondo. Para dar respuesta, y por su estrecha relación con la interrogante señalada en el considerando anterior, se estima necesario acudir en primer lugar a las consideraciones desarrolladas por esta Primera Sala en la contradicción de tesis 128/2018⁵; no sólo por cuanto hace al marco teórico en lo atinente al **a)** comercio electrónico en México, **b)** la firma electrónica y naturaleza jurídica del número de identificación personal, así como **c)** la seguridad en actos de comercio electrónico; sino también respecto del objeto cuya validez resultaba controvertido en dicho precedente, que fundamentalmente involucra la fiabilidad de los servicios que ofrecen las instituciones bancarias por medio de una infraestructura tecnológica.

⁵ Asunto resuelto en sesión de nueve de enero de dos mil diecinueve por unanimidad de cuatro votos de los señores Ministros integrantes de la Primera Sala: Norma Lucía Piña Hernández, Jorge Mario Pardo Rebolledo (Ponente), Alfredo Gutiérrez Ortiz Mena y Juan Luis González Alcántara Carrancá. Ausente: Ministro Luis María Aguilar Morales.

En aquella ocasión correspondió a este Alto Tribunal pronunciarse sobre: i) si el NIP que se asocia a una tarjeta bancaria, con el cual puede realizar operaciones comerciales, constituye una firma electrónica; y ii) a quién le corresponde la carga de la prueba cuando en un juicio se ejerce acción de nulidad de vouchers emitidos por la realización de una operación comercial efectuada con una tarjeta bancaria, y el consentimiento de la persona se emitió mediante un número de identificación personal (NIP).

Los razonamientos esgrimidos en el criterio aludido resultan plenamente aplicables al caso concreto, atendiendo a que constituyen un preámbulo necesario para comprender no sólo el desarrollo de las diversas tecnologías de información que existen en nuestro país y su aplicación al ámbito de los servicios financieros, sino también el reconocimiento de que la creciente demanda de tales servicios ha orillado a las instituciones bancarias a impulsar mecanismos para mantenerse a la vanguardia a fin de evitar el impacto de las vulneraciones derivadas de ciberataques.

No es obstáculo a lo anterior, el hecho de que en la contradicción de tesis 128/2018, este Alto Tribunal se refirió a la demanda de nulidad de los vouchers emitidos con motivo de transferencias autorizadas mediante la utilización de una tarjeta bancaria con el mecanismo CHIP y NIP; mientras que en las controversias mercantiles de las que conocieron los tribunales colegiados, ahora contendientes, versaron sobre la nulidad de transferencias electrónicas de dinero, utilizando el sistema de banca electrónica.

Ello, en virtud de que ambos supuestos encuentran puntos de coincidencia relevantes, en tanto que el objeto de estudio versa sobre

a quién debe corresponder acreditar la fiabilidad del sistema que sirvió para realizar una determinada operación bancaria realizada a través de los medios electrónicos provistos por una institución bancaria.

Por tanto, aun cuando en el presente asunto es necesario desentrañar la naturaleza y objeto de mecanismos diversos a los utilizados en la Contradicción de Tesis 128/2018, dado que no estamos en presencia de transacciones efectuadas a través de tarjetas bancarias provistas con la tecnología CHIP y NIP y la correspondiente digitación de la firma electrónica como exigencia de aprobación; sino frente a transferencias realizadas mediante la utilización del “Sistema de Pagos Electrónicos Interbancarios” (SPEI), es menester hacer referencia a las consideraciones más importantes que rigieron dicho precedente.

En lo relevante y aplicable para el presente asunto, esta Primera Sala sostuvo lo siguiente en la contradicción de tesis 128/2018:

- Que actualmente en la mayoría de las operaciones comerciales se ocupan los medios electrónicos con la finalidad de realizar actos jurídicos entre particulares. Sin embargo, ante la preocupación de que tales actos no consten por escrito, se han ideado mecanismos que otorguen seguridad a las transacciones; buscando una equivalencia funcional entre los actos realizados por medios electrónicos, ópticos o similares con el documento escrito que se exige para ciertos actos jurídicos.
- Que resultaba necesario destacar que la situación fáctica que aduce el cuentahabiente y que puso a consideración de la potestad jurisdiccional es la siguiente: un particular desconoce los cargos hechos a su cuenta derivados de diversas compras efectuadas en un establecimiento comercial, siendo que como medio de pago se utilizó una tarjeta bancaria con chip, que para

efectos de autorización ingresó una firma electrónica (NIP), emitiéndose los vouchers en los que se observó la leyenda: “NIP VERIFICADA o PIN VERIFIED”.

- Que con dicha leyenda puede constatarse que el NIP al introducirlo en una terminal punto de venta, fue verificado por la institución financiera y al resultar coincidente autorizó la operación que derivó en una compraventa, haciendo el cargo correspondiente a la cuenta del usuario.
- Que a partir de un primer acercamiento podría concluirse que, con base en el artículo 1196 del Código de Comercio, la carga de la prueba le correspondería al usuario, en tanto que el destinatario -de conformidad con el artículo 90 bis del Código de Comercio- tiene a su favor la presunción legal de tener como emisario y actuar en consecuencia cuando se haya aplicado el método de identificación acordado. Lo anterior aunado a que, la institución financiera de acuerdo con el artículo 1298-A transcrito, puede ofrecer como medio de prueba el mensaje de datos, y su valoración probatoria dependerá de la fiabilidad del método ocupado para generarlo.
- No obstante, lo anterior, se estimó necesario abordar dos cuestiones antes de distribuir de forma concluyente la carga probatoria: 1. La presunción legal a favor del destinatario, y 2. Los supuestos que podrían originar asuntos como los sucedidos en las ejecutorias contendientes.
- Al respecto, se dijo que si bien el hecho presumido por la ley debe ser aceptado por el juez y por todo el mundo como cierto sin necesidad de que ser probado (mientras no se demuestre lo contrario), **lo cierto es que el hecho del cual se presume aquél y que le sirve de antecedente, sí necesita de mayores elementos de convicción para que el juez lo considere cierto y pueda aplicar esa presunción.**
- En este sentido, se apuntó que si bien el artículo 1196 del Código de Comercio establece que el que niega está obligado a probar cuando su contraparte tiene una presunción legal a su favor,

siendo que en el caso el destinatario del mensaje cuenta con las presunciones establecidas en el artículo 90 bis del mismo Código; lo cierto es que **el hecho del cual se presume aquél y que le sirve de antecedente, sí necesita la plena prueba para que el juez lo considere cierto y pueda aplicar esa presunción, tal como lo establece el artículo 1280 del Código de Comercio.**

- Así, se consideró, previamente a que se le arroje la carga de la prueba al usuario que niega haber firmado electrónicamente el voucher, la institución financiera tiene que probar que el método de identificación acordado con el emisor se aplicó de manera correcta. Máxime si se toma en cuenta la diferencia sustancial entre la creación de la firma electrónica ante la institución financiera, la cual se hace con el propósito de utilizarla para realizar diversos actos, con la creación de un mensaje de datos al cual deberá consignarse la firma electrónica (NIP), que sirve para identificar al firmante en relación con el mensaje de datos e indicar que aprueba la información contenida en el mensaje de datos.
- En el contexto anterior, se precisó que la instauración de mecanismos tecnológicos en las tarjetas bancarias, ha propiciado que existan mayores candados para desincentivar las operaciones fraudulentas, como lo constituye el despliegue de mecanismos como el sistema del Chip y el NIP; pero que no obstante, a la par de los avances técnicos, también se ha acrecentado el uso ocasional malintencionado de recursos similares para burlarlos.
- Que una y otra vez, los clientes se han quejado de transacciones fraudulentas que no realizaron, siendo que los bancos ofrecen – generalmente- la misma respuesta consistente en que los mecanismos instaurados (como el Chip y el NIP) son seguros, por lo que debió existir confusión o descuido por parte del usuario, o está actuando fraudulentamente cuando se disputan las transacciones. No obstante, reiteradamente los bancos se han equivocado, ya que una vulnerabilidad tras otra ha sido descubierta y explotada por criminales, y se ha dejado

principalmente a investigadores de seguridad independientes para descubrir qué está sucediendo y publicarla.

- Por ende, se estimó que en el supuesto en que un usuario aduzca desconocer diversos cargos realizados a su tarjeta bancaria, que fueron autorizados con datos de su tarjeta bancaria y el tecleo de su NIP, corresponderá en un primer momento a la institución financiera demostrar el hecho antecesor al presumible previsto en el artículo 90 bis del Código de Comercio.
- Lo anterior es así, ya que -como se ha explicado- la institución financiera tiene a su favor la presunción de que un emisor envió un mensaje de datos, por lo que podrá actuar en consecuencia cuando: i) haya efectuado el procedimiento acordado cuya finalidad haya sido establecer que el mensaje de datos provenía del emisor, o ii) el mensaje proviniera de un intermediario autorizado con acceso a algún método con la misma finalidad referida.
 - De modo que, si la institución financiera quiere gozar de la presunción legal referente a tener como emisor al que envió el mensaje de datos, deberá probar haber utilizado un procedimiento acordado con el usuario para establecer que el mensaje venía de aquél de conformidad con lo pactado en el contrato. Aunado a que, el artículo 1298-A del Código de Comercio establece que, para valorar la fuerza probatoria del mensaje de datos, se tendrá en cuenta la fiabilidad del método en que haya sido generado.
 - Sobre este aspecto se precisó que lo cuestionado no era fiabilidad del método por el cual se creó la firma, en otras palabras, no se impugna la manera en que la institución creó la firma con el usuario por primera vez, porque en todo caso aquélla al probar que usó un método fiable, con lo que en términos del artículo se trasladaría la carga de la prueba al usuario para contradecir que el método no era fiable, y así probar su dicho, lo único que se estaría resolviendo es una cuestión previa al hecho controvertible en específico, pues se probaría que la fiabilidad del método utilizado para la creación de la firma; sin embargo, **la cuestión**

controvertida es posterior al método de creación inicial de la firma y consiste en saber si el sistema en sí mismo fue vulnerado por algún agente externo.

- En ese sentido, se estimó que corresponde en primer lugar a la institución bancaria probar que utilizó el procedimiento acordado con el usuario para establecer que el mensaje venía de aquél. Al respecto, vale la pena mencionar que en el artículo 313 de las Disposiciones de carácter general aplicables a las Instituciones de Crédito, se establece que las Instituciones deberán solicitar a sus usuarios para la celebración de operaciones o prestación de servicios a través de medios electrónicos dos factores de autenticación a que se refiere el artículo 310, los cuales pueden ser categoría 2, 3 o 4, cuando se pretenda el pago de bienes.
- Por ende, se dijo que la institución financiera prestadora del servicio deberá acreditar los procedimientos de identificación que fueron utilizados durante la transacción y que fueron acordados con el usuario. Asimismo, dado que al utilizar como medio de prueba el propio mensaje de datos, cuyo valor está condicionado a la fiabilidad del procedimiento de creación, entonces la institución deberá demostrar que aquél cumple con los requisitos previstos para la verificación de la fiabilidad de las firmas electrónicas, es decir, que los datos de creación del mensaje en el contexto en que se utilizaron, corresponden exclusivamente al emisor, sin que el sistema en sí mismo haya sido alterado por algún agente externo.
- Aunado a que, como se precisó, los métodos de clonación de datos evolucionan de forma desmesurada, siendo que es responsabilidad de las instituciones financieras dotar de seguridad a los mecanismos por los cuales se realizan operaciones financieras, y en todo caso cuenta con los recursos necesarios para demostrar la ausencia de riesgo en aquéllas.
- Por lo tanto, se dijo que cuando el cuentahabiente niegue haber realizado los pagos que originaron los cargos cuya cancelación demandó, entonces **es la institución bancaria la que tiene la obligación de aportar las pruebas pertinentes con las que se**

acredite que fue el propio usuario quien realizó los mismos, es decir, que fue el emisor de la autorización mediante la firma electrónica; pues no debe perderse de vista que son las instituciones bancarias prestadoras del servicio las que se encuentran en una posición dominante en la relación de consumo, por lo que están obligadas a garantizar la seguridad en todas las operaciones que se lleven a cabo con motivo de los contratos celebrados con sus clientes, pues son ellas las que cuentan con dispositivos y mecanismos que facilitan la aportación de pruebas, al ser las encargadas de la implementación de las medidas de seguridad a efecto de poder verificar no sólo los montos de las disposiciones o los cargos, sino la utilización de la tarjeta que cuenta con mecanismo CHIP y del número de identificación personal de los usuarios.

- En ese sentido, se concluyó que solo una vez que la institución bancaria haya acreditado tales extremos, de conformidad con el artículo 1280 del Código de Comercio, es decir, solo cuando se acredite que no ocurrió una vulneración al sistema durante esa transacción (como podría ser la extracción de información en los mensajes de datos) y que tomó las medidas de seguridad necesarias; entonces la carga de la prueba se le revertirá al usuario quien tendrá el deber de desvirtuar lo aportado por aquélla.

Como se advierte de sus principales consideraciones, en la contradicción de tesis 128/2018, esta Primera Sala determinó que en caso de que se demande la nulidad de los vouchers emitidos con motivo del uso de una tarjeta bancaria cuya autenticación se originó mediante la digitación de un número de identificación personal, es la institución bancaria quien está obligada a ofrecer las pruebas pertinentes que acrediten que fue el propio usuario quien realizó dicha transacción.

Al respecto, se observa que en aquella ocasión se justificó el que debieran ser las instituciones bancarias quienes debieran acreditar tal situación, en los siguientes razonamientos:

- A. Que la firma electrónica del cuentahabiente mediante el tecleo de su número de identificación personal (NIP) acredita presuntivamente la existencia y validez de las transacciones; pero para que el o la juzgadora esté en aptitud de aplicar esa presunción se necesita la exhibición de mayores elementos para demostrar la fiabilidad del método utilizado para la generación de la firma.
- B. En ese sentido, se razonó que las instituciones bancarias prestadoras del servicio son las que se encuentran en una posición dominante en la relación de consumo, por lo que están obligadas a garantizar la seguridad en todas las operaciones que se lleven a cabo con motivo de los contratos celebrados con sus clientes, pues son ellas las que cuentan con dispositivos y mecanismos que facilitan la aportación de pruebas, al ser las encargadas de la implementación de las medidas de seguridad.
- C. Por tanto, se estimó que si la institución financiera quiere gozar de la presunción legal de tener como emisor al que envió el mensaje de datos, debe probar los procedimientos de identificación que fueron utilizados durante la transacción y que fueron acordados con el usuario, de conformidad con lo dispuesto en el artículo 310 de las Disposiciones de carácter general aplicables a las Instituciones de Crédito; así como que esos procedimientos cumplen con los requisitos previstos para la verificación de la fiabilidad de las firmas electrónicas, esto es, que los datos de creación del mensaje en el contexto en que se utilizaron, corresponden exclusivamente al emisor, sin que el sistema en sí mismo haya sido alterado por algún agente externo.
- D. Que no era obstáculo de lo anterior, la regla establecida en el artículo 1196 del Código de Comercio, pues si bien éste establece que corresponde probar al que niega, cuando al hacerlo desconoce la presunción legal que tiene a su favor el colitigante; lo cierto era que el hecho del cual se presume aquél y que le sirve de antecedente, sí requiere de mayores elementos probatorios para que el juez lo considere cierto y pueda aplicar esa presunción.

Ahora bien, para estar en aptitud de dilucidar si la misma conclusión lógica puede alcanzarse en la controversia que nos ocupa, primero, es menester definir algunas cuestiones fundamentales, entre las que se encuentra: a) la banca electrónica, b) el Sistema de Pagos Electrónicos Interbancarios, c) la seguridad de la banca electrónica, d) la regulación de la banca electrónica dentro del marco jurídico nacional; y e) conclusión.

a) La banca electrónica.

Desde sus orígenes, las instituciones bancarias han buscado herramientas que les permitan, además de otorgar mayor agilidad en la realización de sus operaciones, mantener la seguridad de su patrimonio y, sobre todo, el de sus clientes. Inicialmente, la banca electrónica se hizo presente en la sociedad en forma de cajeros automáticos y transacciones telefónicas.

Sin embargo, a partir del desarrollo exponencial de las nuevas tecnologías de la información, los bancos se vieron obligados a lanzar nuevos canales para obtener una ventaja competitiva, reducir sus costos, mejorar la calidad de sus finanzas y servicios, aumentar su base de clientes y mejorar su posición financiera a través de productos innovadores.

Es por ello que, actualmente, los bancos han optado por mantenerse a la vanguardia con la implementación de mecanismos tecnológicos que propician la inclusión, movilidad, accesibilidad y reducción de costos a los usuarios. Entre estos tipos de servicios, se encuentran, la creación de la banca por internet, el uso de la firma electrónica como medio de autorización en transferencias, los sistemas

electrónicos de pagos y los sistemas automatizados o la creación de tokens de seguridad⁶.

El término "*banca por internet*" o "*banca electrónica*" se refiere al uso de internet como canal de distribución remota para servicios bancarios. En otras palabras, la banca en línea es un término general para el proceso mediante el cual un cliente puede realizar transacciones bancarias electrónicamente sin visitar físicamente las sucursales⁷.

Tal opción permite al cliente hacer las transacciones que desee simplemente con iniciar sesión en el sitio web o en la aplicación para teléfonos móviles, con el ingreso de un número de cuenta y contraseña, bajo el entendido de que prácticamente todos los servicios que ofrece la banca en línea son los mismos que se proporcionan en interacciones físicas. Sin embargo, cabe aclarar que aun cuando la banca en línea tiene muchas características en común entre los bancos que las utilizan, también tienen particularidades concretas que cada institución va adoptando para garantizar la seguridad y confiabilidad de sus plataformas, lo que busca ganar la fidelidad de los usuarios.⁸

⁶ Los "token" de seguridad o contraseña única (o de un solo uso) para cuenta, son pequeños dispositivos sin conexión que generan una contraseña para usar cada vez que inicie sesión en banca por internet. Dicha contraseña será única para la cuenta de cada usuario, y generalmente cuenta con una protección que consiste en su modificación automática dependiendo cierta temporalidad (30 segundos aproximadamente). Recuperado del sitio: "<https://www.frandsenbank.com/document-library/documents/business-online-banking-documents/fbtokenbrochure.aspx>"

⁷ Ullah Khan, Hammed. "*E-banking: Online Transactions and Security Measures*". Maxwell Scientific Publication Corp. Research Journal of Applied Sciences, Engineering and Technology. 2014. P. 4056. Recuperado del sitio: <https://maxwellsci.com/msproof.php?doi=rjaset.7.766>

⁸ Como dato estadístico, en nuestro país anualmente se ha incrementado considerablemente el número de usuarios del sistema bancario, a la par de quienes tienen acceso al uso de internet; por lo que el número de usuarios de transferencias electrónicas o banca en línea ha ido en aumento. Por ejemplo, hasta el tercer trimestre de dos mil veinte, las solicitudes de compra enviadas para autorización ascendió a trescientos setenta mil ochocientos treinta y ocho millones de pesos, de las cuales se autorizó el 62%, que constituyen doscientos cuarenta mil cuatrocientos treinta y seis mil millones de pesos. Estadística visible en: "<https://www.condusef.gob.mx/?p=estadisticas>"

Así, la mayoría de los bancos están proporcionando la instalación en línea de plataformas a través de las cuales los usuarios pueden efectuar operaciones diarias para apertura de cuenta, transferir recursos de una cuenta a otra, emisión de tarjetas de crédito, pago y obtención de préstamos y deudas, además de proporcionar a los clientes instalaciones y recursos seguros para comprar en línea.

Para la resolución de la presente contradicción, es menester hacer énfasis en el servicio que ofrecen los bancos denominados “transferencia electrónica”.

Las transferencias electrónicas son un servicio que ofrecen los bancos a sus clientes para que, con cargo a sus cuentas de depósito, puedan instruir pagos electrónicos a otras cuentas bancarias. Tales cuentas pueden estar dentro del mismo banco o en bancos distintos.

Para poder realizar este tipo de transacciones, el usuario debe dar de alta la cuenta del comercio o de la persona a la que va a efectuar el pago, siendo importante corroborar que todos los datos para la transferencia sean correctos.

Cuando la cuenta del comercio electrónico y la del comprador están en el mismo banco, y el pago se realiza a través de una transferencia, a estas se les denomina "transferencias mismo banco", las cuales, en ocasiones generan al ordenante una comisión o porcentaje por la transacción.

Por otro lado, para realizar transferencias de fondos entre cuentas que están en bancos distintos, existen sistemas de pagos que permiten

realizarlas de forma rápida y segura. El Sistema de Pagos Electrónicos Interbancarios (SPEI), es el sistema que liquida la gran mayoría de transferencias entre bancos con mayor celeridad.

b) El Sistema de Pagos Electrónicos Interbancarios.

El Sistema de Pagos Electrónicos Interbancarios (en adelante SPEI) es un sistema desarrollado y administrado por el Banco de México, que permite al público en general realizar pagos electrónicos en cuestión de segundos. Fundamentalmente, consiste en un canal central al que se conectan los participantes, sobre el cual se pretende se carguen sus cuentas con el Banco de México, para permitir el envío y recepción de pagos entre sí, para poder brindar a sus clientes finales el servicio de transferencias electrónicas en tiempo real.

Tal sistema comenzó a operar el trece de agosto de dos mil cuatro. Fundamentalmente consiste en llevar información para indicar si un cliente ordena un pago y, en su caso, identificarlo; y, por otro lado, para instruir al participante receptor que acredite que éste fue hecho a uno de sus clientes.

Entre las entidades que pueden fungir como participantes se encuentran aquellas sujetas a la regulación en el ámbito federal, en materia financiera, supervisadas por el Banco de México, la Comisión Nacional Bancaria y de Valores, la Comisión Nacional de Seguros y Fianzas o la Comisión Nacional del Sistema de Ahorro para el Retiro; así como las dependencias o entidades de la Administración Pública Federal; el Banco de México, en su carácter de fiduciario de fideicomisos; así como las instituciones que operen un sistema

internacional de liquidación de operaciones cambiarias que incluyan al peso como una de las divisas participantes⁹.

Para pagar por SPEI es necesario conocer la Clave Bancaria Estandarizada (CLABE) de la cuenta de destino (18 dígitos), el número de tarjeta de débito (16 dígitos) o, en su caso, el número de teléfono celular (10 dígitos) asociado a la cuenta de la persona o comercio a la que se le va a abonar la cuenta. Cabe destacar que dicho sistema ejecuta con frecuencia un proceso que determina qué pagos pueden liquidarse con los saldos que los participantes tienen en ese momento; sin embargo, no acepta sobregiros en las cuentas, por lo que no hay crédito de parte del Banco Central.

Su funcionamiento es el siguiente:

- I) El cuentahabiente instruye desde su banca electrónica o aplicación móvil a su institución participante los pagos que desea realizar. Esto se hace siguiendo rigurosos controles de seguridad como contraseñas, elementos dinámicos (tokens) y pruebas de posesión de dispositivos (como mensajes a teléfonos móviles pre registrados), entre otros.
- II) El participante valida los elementos de seguridad de la instrucción y guarda evidencia de que realizó esta validación.
- III) El participante prepara las instrucciones de sus clientes, les incluye elementos de seguridad adicionales (sujeto a la

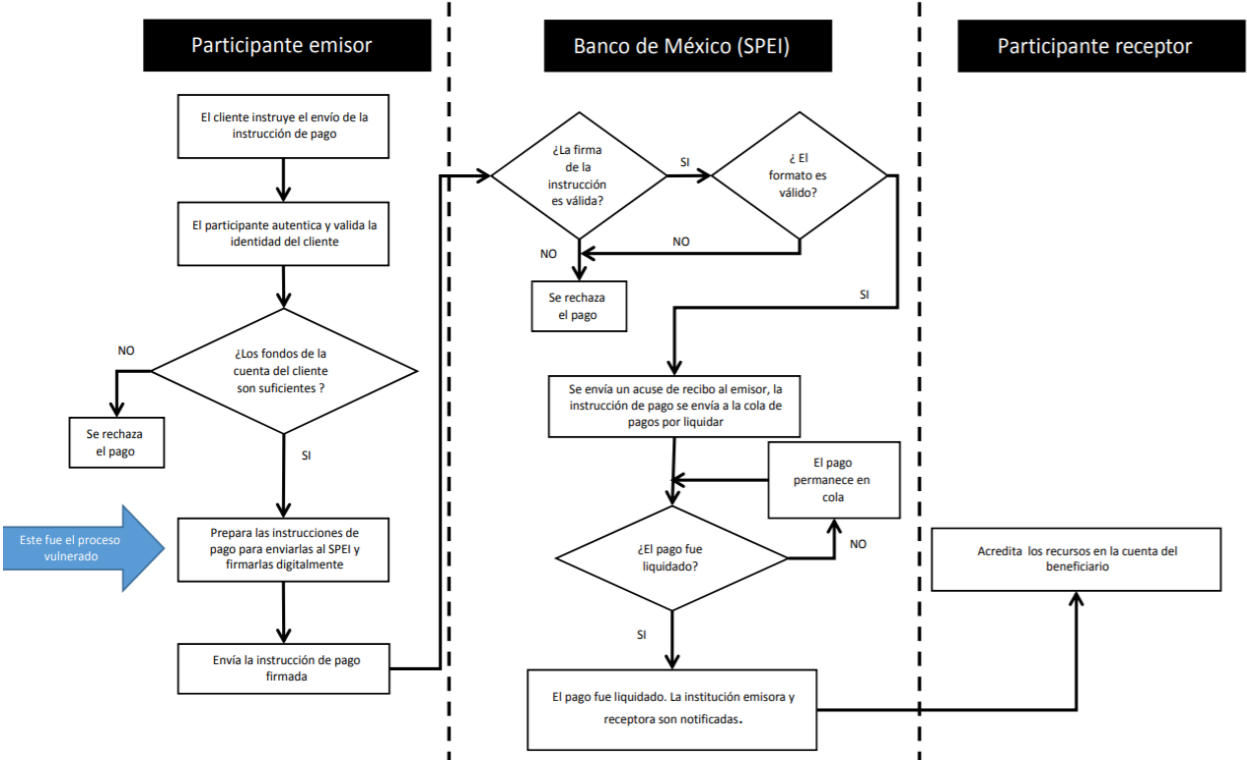
⁹ Características del Sistema de Pagos Electrónicos Interbancarios (SPEI), extraído de la página oficial del Banco de México, en la siguiente dirección electrónica: "https://www.banxico.org.mx/servicios/spei_-transferencias-banco-me.html"

circular 14/2017¹⁰), sobre los cuales únicamente ellos tienen el control, y los envían al SPEI de Banco de México.

- IV) El Banco de México verifica las firmas electrónicas de los participantes, que dan certeza de la integridad de la instrucción de pago, y procede a su procesamiento y posterior liquidación al participante receptor del pago.
- V) Se informa a los participantes involucrados en la transferencia de recursos de la liquidación y el participante receptor del pago acredita los fondos en la cuenta de su cliente y envía al Banco de México la información para generar el Comprobante Electrónico de Pago (CEP).

De manera gráfica, el propio Banco de México lo expone de la forma siguiente:

¹⁰ **Circular 14/2017 relativa a las Reglas del Sistema de Pagos Electrónicos Interbancarios.** Publicada en el Diario Oficial de la Federación el 4 de julio de 2017, incluyendo sus modificaciones dadas a conocer mediante Circulares 5/2018, 11/2018, 18/2018, 3/2019 y 8/2019, publicadas en el referido Diario el 17 de mayo de 2018, 27 de julio de 2018, 24 de diciembre de 2018, 7 de marzo de 2019 y 20 de mayo de 2019, respectivamente.



En cuanto a la seguridad del SPEI, ésta se basa fundamentalmente en mensajes firmados digitalmente. Para ello, los participantes usarán los certificados digitales y las claves de las personas autorizadas, quienes deberán obtenerlas de acuerdo con las normas de la Infraestructura Extendida de Seguridad (IES), del Banco de México.

c) Seguridad de la banca electrónica.

Sobre este aspecto, debe señalarse que, al igual que la vulnerabilidad que representan las transacciones utilizando una tarjeta con mecanismo chip y número de identificación, como fue estudiado en la Contradicción de Tesis 128/2018; la revolución digital que está

transformando la banca por internet también enfrenta desafíos cibernéticos en su funcionamiento.

Existen diversos riesgos asociados a la banca electrónica, ya sean estratégicos, operativos, legales y reputacionales. El riesgo operativo se encuentra estrechamente vinculado con los mecanismos de seguridad que pueden implementarse para evitar vulneraciones a los sistemas establecidos para el correcto desarrollo transaccional; no obstante, con este tipo de riesgo también pudiera verse ligada a la institución en afectaciones legales y reputacionales¹¹. Por ejemplo, cuando se detecta una violación a la seguridad de la plataforma donde se permitiera acceso no autorizado a la información de clientes, no solo expone al banco a verificar la transferencia no reconocida, sino que también puede generar conflictos legales y riesgo en la reputación de la institución por el manejo defectuoso de sus sistemas.

En el presente caso, no se evaluará algún otro tipo de riesgo diferente al operacional que ocurre ante la posibilidad de que exista alguna brecha en los filtros de seguridad de las instituciones que prestan el servicio de banca electrónica.

Ahora bien, las operaciones electrónicas que se realicen por medio de los sistemas provistos por las instituciones bancarias no pueden llegar a denominarse infalibles y, por tanto, mantener una presunción absoluta respecto a su debido funcionamiento.

¹¹ Vrincianu, Marinela y Anica Popa, Liana. *"CONSIDERATIONS REGARDING THE SECURITY AND PROTECTION OF E-BANKING SERVICES CONSUMERS' INTERESTS"*. Academy of Economic Studies, Bucharest, Romania. Amfiteatrou Economic, Vol. XII, número 28, junio 2010. Recuperado de: "<https://core.ac.uk/download/pdf/6492899.pdf>"

Este tipo de sistemas, como todo avance tecnológico, ha demostrado diferentes cualidades para constituirse como una tecnología que vuelve más eficiente la prestación de servicios, pero que no se encuentra libre de riesgos de seguridad en su operación¹². Por ende, como cualquier servicio que dependa de una infraestructura tecnológica, es susceptible de intromisiones directas o indirectas que vician su operación, es necesario analizar el grado del ataque en cuanto a intensidad, habilidad y persistencia.¹³

Incluso, el gran volumen de transacciones digitales significa que los métodos manuales tradicionales de monitoreo y detección de fraude no tienen la capacidad ni la velocidad para enfrentar el desafío al que se enfrentan los bancos en la actualidad¹⁴.

Sobre este aspecto, se han identificado algunos mecanismos en que terceros han dirigido ataques a los sistemas tecnológicos:

A. **Malware.** Es el término simplificado para denotar “malicious code” y consiste en aquel software destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la confidencialidad, integridad o disponibilidad de un sistema de información. Dentro de esta categoría se encuentran principalmente los siguientes tipos:

- Virus: Sección oculta y auto replicante de software informático, que se propaga al infectar (es decir, al

¹² Fernando Pérez Márquez, Documento de Trabajo No. 181, Riesgo Cibernético y Ciberseguridad, Secretaría de Hacienda y Crédito Público, Comisión Nacional de Seguros y Fianzas, 2019, páginas 10 a 12.

¹³ Ullah Khan, Hammed. Op. cit.

¹⁴ Net Guardians. “Digital banking fraud: Best practice for technology-based prevention”. Recuperado de: “<https://netguardians.ch/digital-banking-fraud/>”

insertar una copia de sí mismo en otro programa y convertirse en parte de él). Un virus no puede correr solo; requiere que su programa huésped se ejecute para activarlo.

- Spyware: Software que se instala de forma secreta o subrepticia en un sistema de información para recopilar información sobre individuos u organizaciones sin su conocimiento.
- Adware: Software que reproduce, muestra o descarga automáticamente material publicitario a una computadora después de instalar el software o mientras se utiliza la aplicación. El programa malicioso está diseñado para mostrar publicidades no deseadas en la computadora de la víctima sin su permiso, los pop-ups o anuncios son incontrolables y tienden a comportarse de forma errática, por lo general aparecen muchas veces en la pantalla y resulta tedioso cerrarlos.
- Rootkit: Un conjunto de herramientas utilizadas por un atacante después de obtener acceso al nivel de raíz en un host para ocultar las actividades del atacante en el host y permitirle mantener el acceso de nivel de raíz "root" al host a través de medios secretos. En otras palabras, permite a un pirata informático acceder o controlar de forma remota un dispositivo informático o una red sin estar expuesto. Son difíciles de detectar debido a que se activan incluso antes de que se inicie el sistema operativo del sistema.
- Trojan Horse: Programa de computadora que parece tener una función útil, pero también tiene una función oculta y potencialmente maliciosa que evade los

mecanismos de seguridad, a veces explotando autorizaciones legítimas de una entidad que invoca el programa.

- Worm: Es el término simplificado para denotar “write once, read many”, consiste en un programa informático que puede ejecutarse de forma independiente, puede propagar una versión completa de sí mismo en otros host o redes y puede consumir los recursos de una computadora de manera destructiva. En otras palabras, es un código malicioso que se copia asimismo y se esparce hacia otras computadoras, un sistema o red.
- Ransomware: Es un virus que impide que el usuario acceda a los archivos o programas y para su eliminación se exige pagar un “rescate” a través de ciertos métodos de pago en línea. Una vez pagada la cantidad, el usuario puede reanudar el uso de su sistema.
- Keylogger: Un programa diseñado para registrar qué teclas se presionan en un teclado de computadora que se usa, para obtener contraseñas o claves de cifrado.
- Botnet: Es una red de dispositivos que se ha infectado con software malintencionado, como un virus. Los atacantes pueden controlar una botnet como grupo sin el conocimiento del propietario con el objetivo de aumentar la magnitud de sus ataques. A menudo, una botnet se usa para abrumar a los sistemas en un ataque de denegación de servicio distribuido (DDoS).

B. Phishing. Una técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta en un correo electrónico o en un

sitio web, en la que el perpetrador se hace pasar por un negocio legítimo o una persona con reputación.

C. **Man-in-the-middle attack (MitM).** Un ataque MitM es cuando un atacante altera la comunicación entre dos usuarios, haciéndose pasar por ambas víctimas para manipularlos y obtener acceso a sus datos. Los usuarios no son conscientes de que realmente se están comunicando con un atacante y no entre ellos.

D. **Distributed denial-of-service attack (DDoS).** Un ataque de denegación de servicio inunda sistemas, servidores o redes con tráfico para agotar los recursos y el ancho de banda. Como resultado, el sistema no puede cumplir con solicitudes legítimas. A veces el atacante puede inyectar y ejecutar un código arbitrario mientras realiza un ataque DoS para acceder a la información o ejecutar comandos en el servidor. Este tipo de ataque degrada significativamente el servicio y la calidad experimentada por usuarios legítimos, pues introduce grandes retrasos en la respuesta del sistema¹⁵. Los atacantes también pueden usar múltiples dispositivos comprometidos para lanzar este ataque. Esto se conoce como un ataque de denegación de servicio distribuido.

E. **SQL injection.** Ocurre cuando un atacante inserta código malicioso en un servidor que utiliza SQL (Structured Query Language). Sólo tienen éxito cuando existe una vulnerabilidad de seguridad en el software de una aplicación. Los ataques de

¹⁵ Ullah Khan, Hammed. Op. cit.

SQL exitosos obligan a un servidor a proporcionar acceso o modificar datos.

F. **Zero-day attack.** Un ataque que explota una vulnerabilidad de hardware, o software desconocido anteriormente. El uso de software obsoleto (no parchado), abre oportunidades para que los piratas informáticos criminales aprovechen las vulnerabilidades. Una vulnerabilidad de día cero puede ocurrir cuando una vulnerabilidad se hace pública antes de que el desarrollador haya implementado un parche o una solución.”

Por su parte, en relación con la calidad operacional de banca por internet, The Open Web Application Security Project (OWASP)¹⁶ ha clasificado los riesgos de seguridad en las aplicaciones de red de acuerdo con los ataques exitosos ocurridos.

Entre los ataques informados¹⁷, encontramos los siguientes:

- I) **Injection Flaws.** Los defectos de inyección pueden ocurrir en el lenguaje de consulta estructurado (Structured Query Language SQL) o en el protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol LDAP). La inyección ocurre cuando se envían datos no confiables a un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute de forma no intencionada comandos o acceder a datos no autorizados.

¹⁶ Open Web Application Security Project® (OWASP) es una fundación sin fines de lucro que trabaja para mejorar la seguridad de los softwares, a través de proyectos de código abierto liderados por diversos miembros expertos en desarrollo tecnológico para proteger la web. “<https://owasp.org/#>”

¹⁷ Ullah Khan, Hammed. Op. cit.

- II) **Cross-Site Scripting (XSS).** Se suscitan cada vez que una aplicación toma datos no confiables y envía a un navegador web sin la validación adecuada, para luego escapar. Este tipo de mecanismo permite a los atacantes ejecutar *scripts* en el navegador de la víctima que incluso puede llegar a secuestrar sesiones de usuario, desfigurar sitios web o redirigir al usuario a sitios maliciosos.
- III) **Broken Authentication and Session Management (BA&SM).** Este tipo de funciones posibilitan a los atacantes comprometer contraseñas, claves, tokens de sesión, o explotar otras fallas de implementación para asumir las identidades de otros usuarios. El objetivo de este ataque es apoderarse de una o más cuentas obteniendo los mismos privilegios que el usuario real.
- IV) **Insecure Direct Object References (IDOR).** La referencia de objeto ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, como, un archivo, un directorio o una clave de base de datos. Sin un acceso de control u otra protección, los atacantes pueden manipular estas referencias para acceder a datos no autorizados de otras personas.
- V) **Cross-Site Request Forgery (CSRF).** Este tipo de ataque obliga a iniciar sesión en el navegador de la víctima para enviar una solicitud HTTP falsificada, incluida la *cookie*¹⁸ de sesión de

¹⁸ Las cookies son archivos de texto con pequeños datos, como un nombre de usuario y una contraseña, que se utilizan para identificar su computadora mientras se utiliza una red informática. Las cookies específicas conocidas como cookies HTTP se utilizan para identificar usuarios específicos y mejorar su experiencia de navegación de la red. El navegador almacena cada mensaje en un archivo pequeño, llamado *cookie.txt*; así, al abrir una página en el servidor, su navegador envía la cookie de vuelta, por lo que estos archivos

la víctima y cualquier otra información de autenticación incluida automáticamente, a una aplicación de red vulnerable. Lo anterior permite al atacante obligar al navegador de la víctima a generar solicitudes ilegítimas, aun cuando la aplicación vulnerada las tenga como legítimas.

- VI) **Insecure Cryptographic Storage (ICS).** El almacenamiento criptográfico inseguro consiste fundamentalmente en la inadecuada protección de muchas aplicaciones web de los datos sensibles, como podrían ser los números de tarjetas y las credenciales de autenticación. A partir de ello, el atacante puede robar o modificar dichos datos débilmente protegidos para realizar robo de identidad, fraude con tarjetas de crédito u otros delitos similares.

A partir del marco conceptual esbozado se advierte que los usuarios del sistema de banca electrónica aún enfrentan dificultades en relación con el acceso no autorizado a sus cuentas bancarias.

El conocimiento de los riesgos de seguridad en línea es, a menudo, deficiente por parte de los clientes, lo que facilita los engaños y la divulgación de sus datos confidenciales a grupos delictivos que luego pueden usarse para autenticar transacciones fraudulentas.

Existen alrededor del mundo diversos ejemplos de vulneraciones en la ciberseguridad de las instituciones bancarias, ejemplo de ello, lo constituye el robo masivo suscitado en el Reino Unido respecto de

suelen contener información sobre su visita a la página, así como cualquier información que haya proporcionado voluntariamente, como su nombre e intereses. Recuperado de la Universidad de Indiana (Indiana University), en la liga electrónica siguiente: "<https://kb.iu.edu/d/agwm>"

Tesco Bank en noviembre de dos mil dieciséis, quien sufrió una violación de seguridad en línea en la que se retiraron un total de dos millones y medio de libras esterlinas, de veinte mil de sus ciento treinta y seis mil cuentas corrientes, detectándose actividad sospechosa sobre un porcentaje similar¹⁹.

Nuestro país no es la excepción²⁰. En dos mil dieciocho, el Banco de México reportó que piratas informáticos robaron alrededor de trescientos millones de pesos al crear órdenes fantasmas para transferir fondos a cuentas falsas para luego retirarlos. Lo anterior ocurrió mediante un ciberataque al software aplicativo usado por algunos bancos para conectarse al SPEI, lo que afectó las transferencias electrónicas, confirmándose la realización de operaciones no autorizadas²¹.

¹⁹ Los expertos en tecnología sugirieron que los piratas informáticos habían identificado una debilidad en el sitio web de Tesco Bank y la habían aprovechado para robar miles de detalles de cuentas de clientes que luego se utilizaron para realizar compras en línea. Al descubrir el fraude, Tesco bloqueó temporalmente los pagos en línea de sus clientes de cuenta corriente, mientras continuaba permitiéndoles usar tarjetas para retiros de efectivo, chip y pin, y pagos de facturas. Recuperado de: <https://www.reuters.com/article/us-tesco-bank-idUSKBN1331TX>.

²⁰ Cfr. Reporte en Materia de Ciberseguridad del Banco de México que para el año dos mil diecinueve reportó la existencia de ocho incidentes cibernéticos en el sistema financiero nacional, de los cuales dos se dirigieron al canal de Banca móvil en septiembre de dos mil diecinueve, ocasionado una afectación de treinta y un millones de pesos. El incidente se describió de la siguiente manera: *“Después de iniciar una sesión en un dispositivo móvil con claves robadas a los clientes, los atacantes lograron vulnerar los controles de la aplicación del Banco para enviar transferencias por montos superiores a los permitidos, aprovechando deficiencias en los procesos de validación y control del sistema”*. Asimismo, para el año dos mil veinte, el Banco de México reportó cuatro incidentes cibernéticos, de los cuales dos se dirigieron al servicio de banca por internet. Estos incidentes perpetuados en abril y noviembre se describieron como Ransomware en servidores de un banco comercial, entre los que se identificaron los tipos siguientes MedusaLocker, Sodinokibi, Crysis/Phobos y Emotet. Ambos reportes son consultables en la panga de internet del Banco de México siguiente: <https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html#collapse1>

²¹ Caso SPEI: la cronología del hackeo al sistema financiero mexicano. Recuperado de: <https://expansion.mx/economia/2018/05/18/caso-spei-la-cronologia-del-hackeo-al-sistema-financiero-mexicano>.

Al respecto, cabe destacar que el propio Banco de México ha reconocido que la violación de seguridad ocurrió en la etapa previa a la valoración de formato en la plataforma SPEI, es decir, en la etapa de instrucción de pago y firma digital del banco participante; empero, lo cierto es que, con independencia del momento específico que se haya suscitado el ataque, a partir de su actualización, se logró evidenciar la existencia de nuevas y más eficientes tecnologías para llevar a cabo ciberataques.²²

Ante este panorama, las instituciones financieras que participan en cualquier forma de banca por internet deben tener métodos confiables para autenticar a los clientes, desarrollando sistemas eficaces para salvaguardar su información, a fin de prevenir el fraude electrónico e inhibir el robo de identidades.

Para ello se ha recomendado no solo la implementación de métodos que incluyan el uso de contraseñas y números de identificación, certificados digitales, contraseñas de un solo uso y otros tipos de “tokens”, pues el nivel de protección contra riesgos que ofrece cada una de estas técnicas varía, por lo que es aconsejable adoptar la implementación de diferentes y más novedosas técnicas como podrían ser las características biométricas de los usuarios. Al respecto el Consejo Examinador de Instituciones Financieras Federales (Federal Financial Institutions Examination Council FFIEC), establece que las metodologías de autenticación deben involucrar tres factores básicos: a) algo que el usuario sepa (por ejemplo, contraseña, PIN); algo que el usuario tenga (verbigracia, una tarjeta bancaria); y, algo que sea del

²² Cabe destacar que si bien Banco de México emitió un comunicado sobre el caso en donde anunció medidas en el ámbito tecnológico, operativo y regulatorio para mitigar el riesgo de este tipo de incidentes y la Asociación de Bancos de México (ABM) confirmó que los recursos de los clientes de sus bancos integrantes estaban plenamente protegidos; lo cierto es que el riesgo quedó plenamente evidenciado.

usuario (por ejemplo, características biométricas como una huella dactilar, el iris ocular o el reconocimiento facial).²³

d) La regulación de la banca electrónica dentro del marco jurídico nacional

Precisamente, ante la presencia de estos riesgos, las autoridades han ido adecuando la normatividad aplicable a las instituciones financieras para prever obligaciones específicas en cuanto al establecimiento de mecanismos reactivos y/o preventivos para combatir las prácticas irregulares que pretendan obtener un provecho ilegítimo por medio de la vulneración a estos sistemas electrónicos.

Estas obligaciones encuentran su fundamento en la Ley de Instituciones de Crédito y el Código de Comercio, sin embargo, existen otras disposiciones en las cuales se delinea primordialmente el marco normativo aplicable en relación a las transferencias por mecanismos electrónicos, entre otras, las Disposiciones de carácter general aplicables a las Instituciones de Crédito, por medio del cual la Comisión Nacional Bancaria y de Valores ejerce su función de supervisar y regular a las entidades integrantes del sistema financiero mexicano a fin de procurar su estabilidad y correcto funcionamiento en protección de los intereses del público.

De manera general, la Ley de Instituciones de Crédito en su artículo 52 establece que las instituciones de crédito podrán pactar la

²³ Aunado a ello, señala que los métodos de autenticación que dependen de más de un factor son más difíciles de comprometer. En consecuencia, un método de autenticación multifactorial correctamente diseñado e implementado constituye un elemento disuasorio del fraude muy fiable y potente. Extraído del reporte intitulado "*Authentication in an Internet Banking Environment*", consultable en la liga siguiente: "https://www.ffiec.gov/%5C/pdf/authentication_guidance.pdf"

celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, en donde se establecerá con claridad los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.

Por su parte, dicho reconocimiento se encuentra inmerso en los artículos 80, 89 y 94 del Código de Comercio, donde se establece que, para la formación de actos de comercio, pueden emplearse los medios electrónicos, ópticos o cualquier otra tecnología que se estime necesarios, expresando una serie de definiciones para explicar los mecanismos que pueden utilizarse, entre ellos, la función del mensaje de datos y la expedición entre emisor y destinatario.

De manera particular, la Comisión Nacional Bancaria y de Valores, al emitir las Disposiciones de Carácter General aplicables a las Instituciones de Crédito²⁴, estableció un capítulo específico por lo que

²⁴ Publicadas en el Diario Oficial de la Federación el 2 de diciembre de 2005. Modificadas mediante Resoluciones publicadas en el citado Diario Oficial el 3 y 28 de marzo, 15 de septiembre, 6 y 8 de diciembre de 2006, 12 de enero, 23 de marzo, 26 de abril, 5 de noviembre de 2007, 10 de marzo, 22 de agosto, 19 de septiembre, 14 de octubre, 4 de diciembre de 2008, 27 de abril, 28 de mayo, 11 de junio, 12 de agosto, 16 de octubre, 9 de noviembre, 1 y 24 de diciembre de 2009, 27 de enero, 10 de febrero, 9 y 15 de abril, 17 de mayo, 28 de junio, 29 de julio, 19 de agosto, 9 y 28 de septiembre, 25 de octubre, 26 de noviembre, 20 de diciembre de 2010, 24 y 27 de enero, 4 de marzo, 21 de abril, 5 de julio, 3 y 12 de agosto, 30 de septiembre, 5 y 27 de octubre, 28 de diciembre de 2011, 19 de junio, 5 de julio, 23 de octubre, 28 de noviembre, 13 de diciembre de 2012, 31 de enero, 16 de abril, 3 de mayo, 3 y 24 de junio, 12 de julio, 2 de octubre, 24 de diciembre de 2013, 7 y 31 de enero, 26 de marzo, 12 y 19 de mayo, 3 y 31 de julio, 24 de septiembre, 30 de octubre, 8 y 31 de diciembre de 2014, 9 de enero, 5 de febrero, 30 de abril, 27 de mayo, 23 de junio,

se refiere a la operación de la banca electrónica, dentro del Título Quinto denominado “Otras disposiciones”.

En el Capítulo X “Del uso de la Banca Electrónica”, dicho cuerpo normativo prevé, en primer lugar, la exigencia de las instituciones de implementar mecanismos que permitan la identificación del usuario y su autenticación para poder utilizar el servicio de banca electrónica, en términos de la Sección Segunda “De la identificación del Usuario y la Autenticación en el uso del servicio de Banca Electrónica” del mencionado Capítulo.

Así, a lo largo de los artículos 308 a 313 se establece la forma en que deberá permitirse el inicio de una sesión en el sistema de banca electrónica por el usuario del servicio (artículo 308), los requisitos que deben cumplir el identificador de usuario y los factores de autenticación (artículo 309), los tipos de “factores de autenticación”, clasificados en cuatro categorías según la complejidad del mecanismo (artículo 310), la información mínima que se deberá desplegar a efecto de que los usuario puedan autenticar a la institución bancaria (artículo 311), así como la obligación de utilizar un “factor de autenticación” de una categoría en especial, dependiendo del tipo de transacción (artículos 312 y 313).

Tratándose de transferencias de recursos dinerarios a cuentas destino de terceros u otras instituciones, el artículo 313 del ordenamiento en comento exige que dicha operación sea precedida de un factor de autenticación de categorías 3 o 4, no solo para iniciar la sesión en la cuenta bancaria, sino en cada ocasión que se pretenda

27 de agosto, 21 de septiembre, 29 de octubre, 9 y 13 de noviembre de 2015, respectivamente.

realizar ésta. En términos del artículo 310 estas categorías comprenden lo siguiente: la categoría 3 se compone de información contenida, recibida o generada por medios o dispositivos electrónicos, así como la obtenida por dispositivos generadores de contraseñas dinámicas de un solo uso; por su parte, la categoría 4 corresponde a la información del usuario derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano, patrones en iris o retina y reconocimiento facial, entre otras.

Estas primeras disposiciones a las que se hace referencia dan cuenta de los diversos métodos de autenticación del usuario a efecto de que pueda realizar una operación en el sistema de banca electrónica. Sin embargo, los mecanismos de seguridad no se reducen a la introducción de una serie de claves, sino que se complementan con lo dispuesto en la Sección Tercera “De la operación del servicio de Banca Electrónica” del Capítulo en estudio.

De esta manera, en el artículo 314 se dispone que para la celebración de las operaciones monetarias como lo es la transferencia de recursos dinerarios, las cuentas de destino deben registrarse de forma previa a que se realice la transferencia de dinero; precisándose en el párrafo quinto del precepto citado que, salvo algunas excepciones como las que se registren a través de la Banca Móvil²⁵, “(...) *las cuentas de destino deberán quedar habilitadas después de un periodo*

²⁵ Así como las que dispone el último párrafo del artículo 314 de las Disposiciones, que señala “*Para las Operaciones Monetarias que se realicen a través de Banca Host to Host, Terminales Punto de Venta, Cajeros Automáticos y Pago Móvil, no se requerirá que los Usuarios registren las Cuentas Destino; tampoco para las que se realicen mediante Banca Móvil, siempre que, tratándose de este último, el monto de dichas operaciones sea hasta el equivalente a las de Mediana Cuantía por cada operación*”. Las operaciones de mediana cuantía, en términos del artículo 1º, fracción CXX, inciso c), de las Disposiciones, establece que por estas se entenderán aquéllas de hasta el equivalente en moneda nacional a 1,500 UDIs diarias.

determinado por la propia institución; sin que este sea menor a treinta minutos contados a partir de que se efectuó el registro". Asimismo, en el párrafo sexto se prevé que "(...) las Instituciones p[uedan] habilitar Cuentas Destino registradas por sus Usuarios sin que les sea aplicable el periodo mínimo de tiempo referido en el párrafo anterior, siempre y cuando sea para la realización de Operaciones Monetarias a través de Banca por Internet cuyo monto agregado diario no exceda al equivalente en moneda nacional a las de Baja Cuantía, o bien, el equivalente en moneda nacional a 1,000 UDIs mensuales y obtengan la previa autorización de la Comisión."

De igual forma, el artículo 314 bis establece la posibilidad de registrar cuentas de destino recurrentes, las cuales requerirían un solo factor de autenticación categorías 2, 3 o 4 para realizar una operación, siempre que: i) hayan transcurrido 90 días desde su registro como cuenta destino; ii) en dicho periodo, el usuario hubiere utilizado la cuenta destino al menos en tres ocasiones; y iii) no se hubieren presentado reclamaciones sobre dichas operaciones en el período citado.

Asimismo, destacan para el caso en concreto lo previsto en los artículos 316, 316 bis y 316 bis 1 de las Disposiciones de carácter general aplicables a las Instituciones de Crédito en que se previeron diversas medidas en las que se involucra al usuario en los mecanismos que buscan dotar de certeza sobre la legitimidad en la operación. Como lo es, el que las operaciones que involucren la transferencia de recursos dinerarios a cuentas de terceros u otras instituciones, requieran la notificación a la brevedad al usuario sobre la celebración de las operaciones, tanto antes, como una vez que se éstas llevé a cabo; así como la generación de comprobantes de las operaciones realizadas.

En el mismo sentido, los artículos 316 bis 2 a 316 bis 3 establecen la obligación de adoptar medidas concretas para evitar la intromisión de terceros en el sistema electrónico, entre las que se prevé el establecimiento de periodos máximos en los que puede mantenerse inactiva la sesión en la banca electrónica; y la prohibición de accesos simultáneos a la misma cuenta. De igual manera, se prevén escenarios en que se deban bloquear el uso de las contraseñas y otros factores de autenticación. Por su relevancia se transcribe el artículo 316 bis 3 en comentario:

“Artículo 316 Bis 3.- Las Instituciones deberán establecer procesos y mecanismos automáticos para Bloquear el uso de Contraseñas y otros Factores de Autenticación para el servicio de Banca Electrónica, cuando menos para los casos siguientes:

I. Cuando se intente ingresar al servicio de Banca Electrónica utilizando información de Autenticación incorrecta. En ningún caso los intentos de acceso fallidos podrán exceder de cinco ocasiones consecutivas, situación en la cual se deberá generar el Bloqueo automático.

II. Cuando el Usuario se abstenga de realizar operaciones o acceder a su cuenta, a través del servicio de Banca Electrónica de que se trate, por un periodo que determine cada Institución en sus políticas de operación y de acuerdo con el Medio Electrónico correspondiente, así como en función de los riesgos inherentes al mismo. En ningún caso, dicho periodo podrá ser mayor a un año. Lo anterior, no será aplicable a los servicios de Banca Electrónica ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta.

Las Instituciones podrán Desbloquear el uso de Factores de Autenticación que previamente hayan sido Bloqueados en los casos contemplados en las fracciones I y II anteriores, para lo cual podrán utilizar un Factor de Autenticación Categoría 1 a que se refiere el artículo 310

de las presentes disposiciones, en términos de lo previsto por la fracción III del Artículo 312 de estas disposiciones, o bien, realizar a sus Usuarios preguntas secretas, cuyas respuestas deben conservarse almacenadas en forma Cifrada. Para efectos de lo previsto en el presente párrafo, se entenderá por pregunta secreta al cuestionamiento que define el Usuario o la Institución durante el proceso de contratación del servicio de Banca Electrónica, respecto del cual se genera información como respuesta. Cada pregunta secreta que se defina únicamente podrá ser utilizada en una ocasión.

Con independencia de lo anterior, las Instituciones deberán permitir al Usuario el Restablecimiento de Contraseñas y Números de Identificación Personal (NIP) utilizando el procedimiento de contratación al servicio descrito en el Artículo 307 de las presentes disposiciones.”.

[Énfasis añadido]

Por otra parte, merecen especial mención las adiciones que sufrieron dichas disposiciones mediante la reforma publicada en el Diario Oficial de la Federación de veintisiete de enero de dos mil diez. En este acto se adicionaron al referido Capítulo X del Título Quinto, las Secciones Cuarta “*De la seguridad, confidencialidad e integridad de la información transmitida, almacenada o procesada a través de Medios Electrónicos*” y Quinta “*Del monitoreo, control y continuidad de las operaciones y servicios de Banca Electrónica*”.

En estas secciones que comprenden del artículo 316 bis 10 al 316 bis 12 y del 316 bis 13 al 316 bis 22, se impusieron subsecuentes obligaciones a las instituciones financieras de implementar sistemas de seguridad en la prestación del servicio de banca electrónica.

Cabe señalar que, en el considerando del decreto referido, la autoridad emisora motivó dichas adiciones de la siguiente manera:

“Que en atención al constante desarrollo de nuevas tecnologías y al avance de las existentes, las cuales generan nuevos riesgos y desafíos, resulta conveniente actualizar los requisitos que deberán observar las instituciones de crédito que convengan con el público la celebración de operaciones y la prestación de servicios mediante la utilización de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, **a fin de fortalecer la seguridad y confidencialidad de la información transmitida, almacenada o procesada a través de los citados medios, contando con mecanismos que controlen la integridad de dicha información y la continuidad de los servicios;**

Que es conveniente **actualizar los mecanismos para la identificación de los clientes** de las instituciones de crédito, que sean usuarios de medios electrónicos a través de los cuales se realicen operaciones financieras, así como **determinar las responsabilidades correspondientes a la utilización de los medios mencionados, a fin de prevenir la realización de operaciones irregulares o ilegales que puedan resultar en una afectación a la situación financiera de las instituciones de crédito o de sus clientes,** y

Que de acuerdo con las mejores prácticas internacionales, resulta necesario **definir controles específicos que deberán observar las instituciones de crédito de acuerdo con el grado de riesgo en la realización de operaciones a través del uso de medios electrónicos,** tales como operaciones en cajeros automáticos, pagos mediante terminales punto de venta, pagos y operaciones mediante teléfonos móviles, operaciones mediante banca por Internet, operaciones a través del servicio host to host, operaciones mediante banca telefónica audio respuesta y voz a voz u otros medios electrónicos, a fin de proteger tanto a los usuarios como a las propias instituciones de crédito, ha resuelto expedir la siguiente:...”.

[Énfasis añadido]

En ese tenor, resulta evidente que la propia Comisión Nacional Bancaria y de Valores ha considerado los riesgos de seguridad un aspecto que puede llegar a afectar la situación financiera no solo de las instituciones, sino de los usuarios mismos. De ahí que ha estimado relevante actualizar los mecanismos de identificación de los clientes, así como *“definir controles específicos que deberán observar las instituciones de crédito de acuerdo con el grado de riesgo en la realización de operaciones a través del uso de medios electrónicos”*.

La referencia a esta normativa que ha precedido resulta, por tanto, de vital trascendencia para el estudio que aquí se emprende, pues permite dar cuenta, por un lado, de los riesgos de seguridad en los sistemas bancarios electrónicos que ha advertido la autoridad supervisora el sistema financiero y, por otra parte, la previsión de una obligación de cuidado a cargo de las instituciones bancarias respecto de los servicios ofrecidos a través de la banca electrónica, misma que se concretiza en procedimientos específicos bajo las cuales deben llevarse a cabo las operaciones en la banca electrónica.

Con base en lo anterior, y en la línea de lo que esta Primera Sala señaló al resolver la Contradicción de Tesis 128/2018, la presunción en el sentido de que las transferencias mediante mecanismos electrónicos son infalibles, y por ende, que debe trasladarse la carga de la prueba al usuario del servicio bancario, no puede actualizarse en atención a que como ha quedado de manifiesto, actualmente se conocen diversas maneras de poder obtener fraudulentamente datos de los clientes o vulnerarse contenido electrónico para realizar operaciones fraudulentas; de ahí que la institución bancaria es quien debe de acreditar que los procedimientos de identificación que fueron utilizados

durante la transacción y que fueron acordados con el usuario fueron emitidos correctamente, además de la fiabilidad del procedimiento que se utilizó para autorizar la transacción, máxime si consideramos que el banco cuenta con la infraestructura para generar la evidencia presentada ante los órganos jurisdiccionales.

e) Conclusión.

Ante el escenario descrito, esta Primera estima que no puede presumirse la fiabilidad de la banca electrónica a partir de la mera acreditación de que una transferencia electrónica de dinero se llevó a cabo utilizando un determinado mecanismo de autenticación por parte del usuario. A juicio de este Alto Tribunal, dicha presunción solamente se puede obtener una vez que la institución bancaria demuestre haber seguido el procedimiento exigido normativamente para la realización de la operación de que se trate.

Lo expuesto anteriormente permite concluir que tratándose de una controversia en que resulte controvertida la realización de una operación de transferencia de dinerario a una cuenta de un tercero u otra institución bancaria, corresponde a la institución bancaria acreditar que la operación se realizó de acuerdo a los protocolos exigidos por las Disposiciones de carácter general, aplicables a las instituciones de crédito, emitidas por la Comisión Nacional Bancaria y de Valores, publicadas en el Diario Oficial de la Federación el dos de diciembre de dos mil cinco. Siendo que la mera acreditación de que se ingresaron los medios de autenticación conocidos como las claves y contraseñas para autorizar las operaciones, corresponde a uno de los elementos que deben llevar a dicha convicción.

De ahí que, cuando resulte controvertida la validez de una transacción que tenga por objeto la transferencia de recursos dinerarios a cuentas de terceros u otras instituciones bancarias, no basta con la acreditación de que se introdujeron las claves o contraseñas para acceder al sistema electrónico, con independencia de la categoría que les correspondiera; sino que la institución bancaria deberá demostrar que dicha operación cumplió igualmente con el procedimiento previsto en las Disposiciones de carácter general aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores, concretamente, que el mecanismo de autenticación correspondía al de la cuantía y formato de la operación, la emisión del comprobante y notificación al usuario de la operación respectiva, el debido seguimiento de los plazos establecidos para el registro de una cuenta destinataria, entre otros que se puedan advertir de las disposiciones antes citadas, según corresponda al monto y canal por el que se lleve a cabo la operación.

Sobre este aspecto cabe precisar que en estas circunstancias lo cuestionado no es propiamente la fiabilidad del método por el cual se crearon las claves de autenticación durante la contratación del servicio de banca electrónica a efecto de que el usuario pudiera ingresar a este sistema electrónico. En cambio, la carga probatoria a la que aquí se hace referencia es la de acreditar que el sistema dispuesto por la institución bancaria operó bajo los protocolos establecidos en las Disposiciones de carácter general aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores, al momento en que se llevó a cabo la transferencia de recursos dinerarios, y que, por tanto, el sistema en sí mismo no fue vulnerado por algún agente externo.

Sin que la conclusión alcanzada contravenga lo dispuesto en el artículo 1196 del Código de Comercio, en que se obliga a probar al que niega, cuando al hacerlo desconoce una presunción legal. Pues si bien la transferencia electrónica puede contar con una presunción de fiabilidad en favor de la institución financiera; es necesario que el hecho del cual se presume aquél y que le sirve de antecedente, se funde en mayores elementos probatorios para que el juez lo considere cierto y pueda aplicar esa presunción, a saber, el debido siguiente de los protocolos establecidos en las Disposiciones de carácter general aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores de acuerdo al tipo de operación de que se trate.

El criterio al que se ha arribado criterio se sustenta también en la carga de la prueba prevista precisamente en los artículos 1194, 1195 y 1196 del Código de Comercio, en que se impone la demostración de los hechos controvertidos a la parte que tenga mayor facilidad para aportar los medios conducentes y no a la que se pueda ver en mayores dificultades o en la imposibilidad para hacerlo, la cual encuentra una aplicación especial, tratándose del caso de los consumidores.

De modo que, en las circunstancias concretas, la carga de la prueba implique que sea la parte que ostenta una posición dominante en la relación de consumo la que deba acreditar el funcionamiento en las condiciones debidas. Siendo que la tecnicidad de los sistemas digitales por medio de los cuales se presta el servicio de la banca electrónica representaría un obstáculo excesivo a efecto de que el usuario del servicio pudiera demostrar su pretensión. A diferencia de ello, las instituciones prestadoras del servicio de banca electrónica se

encuentran obligadas a contar con la infraestructura y profesionalización en términos del artículo 316 bis 18 de las Disposiciones de mérito.²⁶

Es a partir de lo anterior, que esta Primera Sala estima que las instituciones bancarias deben ser las que acrediten que el sistema de banca electrónica hubiere operado de acuerdo a la normatividad establecida al momento de llevar a cabo la operación impugnada. Pues, a diferencia de los usuarios, las instituciones financieras cuentan con mayor facilidad para acceder a la información relevante que dé cuenta de las operaciones controvertidas, en atención a la obligación de resguardo de la información, que le asiste en términos de la Sección Quinta, del Capítulo X, de las Disposiciones de carácter general aplicables a las Instituciones de Crédito.

Sobre este punto, debe acudirse a lo dispuesto en el artículo 316 bis 14 de la sección referida, en el cual se establece la obligación de las instituciones bancarias de mantener bases de datos de todas las operaciones no reconocidas que se realicen utilizando el sistema de banca electrónica, de las cuales debe conservar determinada información básica por cinco años a partir de su registro siendo éstos: “(...) [el] *folio de reclamación, fecha de reclamación, causa o motivo de la reclamación, fecha de la operación, cuenta origen, tipo de producto, servicio de Banca Electrónica en el que se realizó la operación, importe, estado de la reclamación, resolución, fecha de resolución, monto abonado, monto recuperado y monto quebrantado*”.

²⁶ “**Artículo 316 Bis 18.-** Las Instituciones estarán obligadas a contar con áreas de soporte técnico y operacional, integradas por personal capacitado, las cuales se encargarán de atender y dar seguimiento a las incidencias que tengan sus Usuarios del servicio de Banca Electrónica, así como a eventos de seguridad relacionados con el uso de Medios Electrónicos.”.

De manera más puntual, el artículo 316 bis 15 prevé la obligación de que las instituciones prestadoras del servicio generen registros, bitácoras, huellas de auditoría de todas las operaciones y servicios bancarios realizados a través de medios electrónicos; ello como se advierte de su propia redacción:

“Artículo 316 Bis 15.- Las Instituciones deberán generar registros, bitácoras, huellas de auditoría de las operaciones y servicios bancarios realizados a través de Medios Electrónicos y, en el caso de Banca Telefónica Voz a Voz, adicionalmente grabaciones de los procesos de contratación, activación, desactivación, modificación de condiciones y suspensión del uso del servicio de Banca Electrónica, debiendo observar lo siguiente:

I. Las bitácoras deberán registrar cuando menos la información siguiente:

a) Los **accesos** a los Medios Electrónicos **y las operaciones o servicios realizados por sus Usuarios**, así como el acceso a dicha información por las personas expresamente autorizadas por la Institución, incluyendo las consultas efectuadas.

b) La fecha y hora, número de cuenta origen y Cuenta Destino y demás información que permita identificar el mayor número de elementos involucrados en el acceso y operación en los Medios Electrónicos.

c) Los datos de identificación del Dispositivo de Acceso utilizado por el Usuario para realizar la operación de que se trate.

d) En el caso de Banca por Internet, deberán registrarse **las direcciones de los protocolos de Internet o similares**, y para los servicios de Banca Electrónica en los que se utilicen Teléfonos Móviles o fijos, deberá registrarse el número de la línea del teléfono en el caso de que esté disponible.

Las bitácoras, incluyendo las grabaciones de llamadas de Banca Telefónica Voz a Voz, deberán ser almacenadas de forma segura por un periodo mínimo de ciento ochenta días naturales y contemplar mecanismos para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

Las bitácoras a que se refiere la presente fracción, deberán ser revisadas por las Instituciones en forma periódica y en caso de detectarse algún evento inusual, deberá reportarse a los Comités de Auditoría y de Riesgos, conforme se establece en el último párrafo del Artículo 316 Bis 19 de las presentes disposiciones.

II. Deberán contar con mecanismos para que la información de los registros de las bitácoras en los diferentes equipos críticos de cómputo y telecomunicaciones utilizados en las operaciones de Banca Electrónica sea consistente.

La información a que se refiere el presente Artículo deberá ser proporcionada a los Usuarios que así lo requieran expresamente a la Institución mediante sus canales de atención al cliente, en un plazo que no exceda de diez días hábiles, siempre que se trate de operaciones realizadas en las propias cuentas de los Usuarios durante los ciento ochenta días naturales previos al requerimiento de la información de que se trate. En caso de grabaciones de voz no se entregará copia de la grabación, solo se permitirá su audición, debiendo proporcionar una transcripción de la misma si es requerida por el Usuario.”

[Énfasis añadido]

Desde esta perspectiva, en que el consumidor se encuentra en una posición de desventaja frente al prestador del servicio bancario en línea, al no contar con los mecanismos tecnológicos necesarios a los que sí puede acceder la institución bancaria; debe agregarse la resistencia que esta última podría poner cuando se ofreciera alguna prueba por parte del cliente, a fin de revisar la estructura y conformación

de sus servidores, pues no debemos perder de vista que dicha data sensible se encuentra bajo un resguardo riguroso al que no puede tener acceso cualquier persona.

En ese sentido, a fin de dilucidar este tipo de controversias los jueces requieren una evaluación integral de quién fue quien efectuó la transacción o el posible defraudador en ese contexto, es decir, si se trató de un tercero que utilizó credenciales o extrajo datos del cliente para efectuar las operaciones o, en su defecto, si el usuario fue el que efectuó las transacciones, o en todo caso, perdió de vista el deber de cuidado que debe tener sobre su información personal. Por tanto, quien está en aptitud de allegarse y verificar esa información, es el propio banco, pues si a su juicio, el sistema no refleja algún movimiento extraordinario adicional al de la transferencia, así debe evidenciárselo al juzgador; máxime que resultaría sumamente improbable que dichas instituciones permitieran el acceso a los controles internos de su sistema a aquellos clientes que demandaran la nulidad de los cargos, como por ejemplo al sistema de tarjetas inteligentes para conexiones o módulos de seguridad de hardware o software.

De ahí que, se insiste, la mera exhibición del registro en que se advierta la operación cuestionada, en ausencia de elementos que permitan verificar que se cumplieron con los protocolos establecidos no se estima suficiente para acreditar la validez de la transacción. Siendo que si la institución bancaria tuviere conocimiento de cualquier incidente que pudiera haber comprometido los datos del cuentahabiente, así deberá declararlo.

Se estima entonces que, **una vez acreditado que se siguió debidamente el procedimiento normativamente exigido de la**

institución financiera para la operación impugnada y que no se tuvo conocimiento de incidentes que comprometieran los datos del cuentahabiente, no deberá además imponérsele a la institución financiera la carga de demostrar la fiabilidad abstracta del sistema. Ello, en tanto que la fiabilidad de la operación quedará presumida una vez que se verifique el debido cumplimiento del procedimiento previsto normativamente, de acuerdo con el tipo, cuantía y canal de la operación, bajo el entendido que no existió tipo de vulneración alguna.

Esto es, tampoco podría llegarse al extremo de exigir de la institución financiera demostrara la fiabilidad genérica de todo su sistema ante cualquier tipo de riesgo que no se hubiere llegado a materializar. En el entendido de que, por la naturaleza mercantil en la que se enmarca la controversia, si bien les asiste legitimación a los usuarios del servicio financiero para reclamar el indebido cumplimiento de las obligaciones normativas a cargo de las instituciones bancarias; no corresponde en esta instancia revisar el absoluto cumplimiento de las obligaciones en materia de ciberseguridad que asisten a dichas entidades en la operación de la banca electrónica, sino únicamente aquellas que permitieran identificar una irregularidad al momento de que llevara a cabo la operación controvertida y con ello acreditar la nulidad de la operación que se reclama.

Aunado a lo anterior, no se considera que la carga impuesta resulte excesiva para las instituciones del sector; fundamentalmente, en tanto que la asignación particular de dicha carga probatoria se encuentra además justificada en la protección reforzada que asiste a los consumidores. En este sentido, si bien existe un régimen especial en que se regula la protección de los consumidores de la banca o

propiamente los usuarios del servicio financiero; ello no limita la protección que deba asistirles en el presente caso.

Ello, pues resulta evidente que los servicios financieros a que se hace referencia, encuadran en una relación de consumo en que los usuarios del servicio tienen la calidad de consumidores, y las instituciones bancarias la calidad de proveedoras del servicio. De manera tal que, si bien la protección de los usuarios encuentra su cauce en una legislación especial, estos no pierden su calidad de consumidores, ni la protección multifacética que les asiste en términos del artículo 28 de la Constitución Política de los Estados Unidos Mexicanos. Alcance que se extiende a todas las vertientes en que pueda llegar a derivar una relación de consumo, como lo es la reivindicación de sus derechos en la vía judicial. Así, la diferencia formal en la protección de los derechos de los usuarios del servicio financiero, no pueda llegar a excluir, *a priori*, los principios y garantías establecidos en favor de los consumidores en general.

Sobre este aspecto, resulta relevante señalar que esta Primera Sala se pronunció al resolver el juicio de amparo directo en revisión 5771/2015²⁷, en que estableció que la protección de los consumidores no es exclusiva del ámbito administrativo; sino que ésta incluye otras vertientes como son la civil y la mercantil, en tanto que, las relaciones de consumo se sirven de instrumentos normativos e instituciones jurídicas de naturaleza civil y/o mercantil para adoptar una estructura e identidad jurídicas, pero siempre quedan sometidas (en mayor o menor medida) al régimen especial de protección al consumidor que el texto

²⁷ Resuelto en sesión de veinticuatro de mayo de dos mil diecisiete por unanimidad de cuatro votos de los señores Ministros Arturo Zaldívar Lelo de Larrea (Ponente), Jorge Mario Pardo Rebolledo, Alfredo Gutiérrez Ortiz Mena y Ministra Norma Lucía Piña Hernández.

constitucional establece para ese tipo especial de relación derivada del acto de consumo y del rol de consumidor.²⁸

Por lo expuesto, debe prevalecer con carácter de jurisprudencia, en términos de los artículos 216, párrafo segundo, 217 y 225 de la Ley de Amparo, la sustentada por esta Primera Sala de la Suprema Corte de Justicia de la Nación, bajo el rubro y texto siguientes:

TRANSFERENCIAS ELECTRÓNICAS BANCARIAS. CUANDO SE RECLAME SU NULIDAD, CORRESPONDE A LA INSTITUCIÓN BANCARIA DEMOSTRAR QUE SE SIGUIERON LOS PROCEDIMIENTOS ESTABLECIDOS NORMATIVAMENTE PARA ACREDITAR SU FIABILIDAD.

HECHOS: Los Tribunales Colegiados de Circuito contendientes sostuvieron posturas distintas respecto a quién correspondía demostrar, en un juicio de naturaleza mercantil, la fiabilidad del mecanismo por el cual se efectuaron transferencias electrónicas de recursos mediante la utilización de plataformas digitales; así, uno estimó que cuando el cuentahabiente niega haber dado su autorización al banco para realizar la transferencia y la institución de crédito afirma que sí recibió la instrucción, corresponde al primero demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad y, por tanto, que su cuenta fue sabotada electrónicamente; mientras que el otro sostuvo lo contrario, es decir, que corresponde a la institución bancaria soportar la carga probatoria de acreditar que las mismas se

²⁸ Lo anterior se refleja en la tesis 1a. CCCXIII/2018 (10a.), de rubro: “**DERECHO FUNDAMENTAL A LA PROTECCIÓN DE LOS INTERESES DEL CONSUMIDOR. SU ALCANCE SE PROYECTA A TODAS LAS VERTIENTES JURÍDICAS QUE ENMARCAN LAS RELACIONES DE CONSUMO.**”. Visible en el Semanario Judicial y su Gaceta. Décima Época, Primera Sala, Aislada, Libro 61, Diciembre de 2018, Tomo I, Página: 306.

realizaron mediante el uso de los elementos de seguridad empleados para garantizar la certeza de las operaciones.

CRITERIO JURÍDICO: La Primera Sala de la Suprema Corte de Justicia de la Nación determina que no puede presumirse la fiabilidad de la banca electrónica a partir de la mera acreditación de que una transferencia se llevó a cabo utilizando un determinado mecanismo de autenticación por parte del usuario. Al respecto, se establece que dicha presunción solamente se puede obtener una vez que la institución bancaria demuestre haber seguido el procedimiento exigido por las Disposiciones de Carácter General, aplicables a las Instituciones de Crédito, emitidas por la Comisión Nacional Bancaria y de Valores. En ese sentido, una vez acreditado que se siguió debidamente el procedimiento normativamente exigido de la institución financiera para la operación impugnada y que no se tuvo conocimiento de incidentes que comprometieran los datos del cuentahabiente, sólo entonces la carga de la prueba se le revertirá al usuario quien tendrá el deber de desvirtuar lo aportado por aquélla.

JUSTIFICACIÓN: Las disposiciones aludidas establecen la previsión de contenidos mínimos para el funcionamiento de la banca electrónica tratándose de las transferencias de recursos, dentro de los que destacan: a) la introducción de mecanismos complejos de autenticación del usuario divididas en cuatro categorías; b) el establecimiento de operaciones con las cantidades dinerarias máximas que pueden llevarse a cabo bajo determinado medio de autenticación; c) la necesidad de registrar previamente las cuentas de destino, así como el periodo mínimo que debe transcurrir antes de poder realizar la transferencia, según sea el caso; y, d) la obligación de generar comprobantes y notificar al usuario de las transacciones. Sin embargo,

a partir de que actualmente se conocen diversas maneras de poder obtener fraudulentamente datos de los clientes o vulnerarse contenido electrónico para realizar operaciones sin el consentimiento de los usuarios, la presunción en el sentido de que las transferencias mediante mecanismos electrónicos son infalibles no puede prosperar, por lo que no es posible trasladar, en un primer momento, la carga de la prueba al usuario del servicio; máxime si se considera la tecnicidad de los sistemas digitales por medio de los cuales se presta el servicio de la banca electrónica lo que representa un obstáculo excesivo a efecto de que el usuario del servicio pudiera demostrar su pretensión, además de que el banco es quien cuenta con la infraestructura necesaria para generar la evidencia presentada ante los órganos jurisdiccionales. De manera tal que la institución financiera es quien debe acreditar que los procedimientos de identificación que fueron utilizados durante la transacción y que fueron acordados con el usuario se emitieron correctamente, además de la fiabilidad del procedimiento que se utilizó para autorizar la transacción. Consecuentemente, una vez acreditado que se siguió el procedimiento normativamente exigido de la institución financiera para la operación impugnada y que no se tuvo conocimiento de incidentes que comprometieran los datos del cuentahabiente, sólo entonces la carga de la prueba se revertirá al usuario quien tendrá el deber de desvirtuar lo aportado por aquélla, sin que lo anterior implique la imposición a los bancos de una carga imposible consistente en la demostración de la fiabilidad abstracta de todo su sistema ante cualquier tipo de riesgo, sino sólo de aquellos que se pudieran llegar a materializar.

Por lo expuesto y fundado, se resuelve:

PRIMERO. Sí existe la contradicción de tesis a que este expediente se refiere, en los términos del considerando cuarto del presente fallo.

SEGUNDO. Debe prevalecer con carácter de jurisprudencia, el criterio sustentado por esta Primera Sala de la Suprema Corte de Justicia de la Nación, en los términos de la tesis redactada en el último considerando de la presente resolución.

TERCERO. Dese publicidad a la tesis jurisprudencial que se sustenta en la presente resolución, en términos del artículo 219 de la Ley de Amparo.

Notifíquese; con testimonio de esta resolución a los Tribunales Colegiados contendientes; y, en su oportunidad, archívese este expediente como asunto concluido.

Así lo resolvió la Primera Sala de la Suprema Corte de Justicia de la Nación, por unanimidad de cinco votos de las Señoras y los Señores Ministros: Norma Lucía Piña Hernández, Juan Luis González Alcántara Carrancá, Jorge Mario Pardo Rebolledo (Ponente), Alfredo Gutiérrez Ortiz Mena y Presidenta Ana Margarita Ríos Farjat.

Firman la Ministra Presidenta de la Primera Sala y el Ministro Ponente con el Secretario de Acuerdos que autoriza y da fe.

PRESIDENTA DE LA PRIMERA SALA

MINISTRA ANA MARGARITA RÍOS FARJAT

PONENTE

MINISTRO JORGE MARIO PARDO REBOLLEDO

SECRETARIO DE ACUERDOS DE LA PRIMERA SALA

MTRO. RAÚL MENDIOLA PIZAÑA

En términos de lo previsto en los artículos 113 y 116 de la Ley General de Transparencia y Acceso a la Información Pública; 110 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública; y el Acuerdo General 11/2017, del Pleno de la Suprema Corte de Justicia de la Nación, publicado el dieciocho de septiembre de dos mil diecisiete en el Diario Oficial de la Federación, en esta versión pública se suprime la información considerada legalmente como reservada o confidencial que se encuentra en esos supuestos normativos.