Reseña de la Contradicción de Tesis 206/2020

Ministro Ponente: Jorge Mario Pardo Rebolledo
Secretario de Estudio y Cuenta: Jorge Arriaga Chan Temblador
Primera Sala de la Suprema Corte de Justicia de la Nación

"CUANDO SE RECLAME LA NULIDAD DE UNA TRANSFERENCIA ELECTRÓNICA CORRESPONDE A LA INSTITUCIÓN BANCARIA ACREDITAR SU FIABILIDAD"

En octubre de 2020, los Magistrados integrantes del Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito denunciaron la posible contradicción de tesis entre el criterio que emitieron y el sustentado por el Primer Tribunal Colegiado en Materia Civil del Décimo Sexto Circuito al resolver, respectivamente, diversos juicios de amparo directo.

El punto jurídico a dilucidar en la contradicción de tesis consistió en definir si debe ser el cuentahabiente o la institución bancaria quien debe 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.

I. Contradicción de criterios

Por una parte, el Primer Tribunal Colegiado en Materia Civil del Décimo Sexto Circuito sostuvo 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 saboteada electrónicamente.

En cambio, el Décimo Quinto Tribunal Colegiado en Materia Civil del Primer Circuito 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.

Una vez admitida la contradicción de tesis por el Alto Tribunal, se determinó la competencia de la Primera Sala para conocer de la misma y se ordenó turnarla a la ponencia del señor **Ministro Jorge Mario Pardo Rebolledo** para la elaboración del proyecto de resolución correspondiente, el cual se aprobó en la sesión del 17 de marzo de 2021.

II. Análisis de la Primera Sala de la Suprema Corte de Justicia de la Nación

La Primera Sala estimó necesario acudir a las consideraciones que desarrolló al resolver la diversa contradicción de tesis 128/2018,[1] en la cual 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 a través del mecanismo denominado CHIP y NIP, es la institución bancaria la que está obligada a ofrecer las pruebas pertinentes que acrediten que fue el propio usuario quien realizó dicha transacción, es decir, se justificó el que debieran ser las instituciones bancarias las que debieran acreditar tal situación.

Explicó que para dilucidar si es aplicable la misma conclusión a la que llegó en aquella contradicción de tesis, era necesario definir algunas cuestiones fundamentales.

---

[1] De dicha contradicción derivó la Tesis: 1a./J. 16/2019 (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 66, Tomo II, mayo de 2019, página 1228, registro digital: 2019919, 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 DEL NÚMERO DE IDENTIFICACIÓN PERSONAL (NIP) EN DISPOSITIVOS DENOMINADOS 'TERMINAL PUNTO DE VENTA'."

a) Banca electrónica

La Primera Sala destacó que los bancos han implementado mecanismos tecnológicos tendientes a la inclusión, movilidad, accesibilidad y reducción de costos a los usuarios, entre los cuales se encuentra 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 seguridad.

Precisó que el término "banca por internet" o "banca electrónica" se refiere al uso de internet como canal de distribución remota para servicios bancarios, es decir, 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 sucursales.

Señalado lo anterior, la Primera Sala destacó que, para efectos de la resolución, era necesario hacer énfasis en las "transferencias electrónicas", que 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.

b) Sistema de Pagos Electrónicos Interbancarios

La Primera Sala refirió que para realizar transferencias de fondos entre cuentas que están en bancos distintos, existen sistemas de pagos que permiten realizarlas de forma rápida y segura, entre ellos, el Sistema de Pagos Electrónicos Interbancarios (SPEI), que es el sistema que liquida la gran mayoría de transferencias entre bancos con mayor celeridad.

Precisó que el SPEI es un sistema desarrollado y administrado por el Banco de México (BM), que permite al público en general realizar pagos electrónicos en cuestión de segundos, de manera general, consiste en un canal central al que se conectan los participantes, sobre el cual se pretende que se carguen sus cuentas con el BM, 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.

Respecto a la seguridad del SPEI, la Primera Sala sostuvo que, fundamentalmente, se basa en mensajes firmados digitalmente, para lo cual, los participantes

usan certificados digitales y claves de las personas autorizadas, que obtienen de acuerdo con las normas de la Infraestructura Extendida de Seguridad (IES), del BM.

c) Seguridad de la banca electrónica

La Primera Sala hizo notar que las operaciones electrónicas que se realicen por medio de los sistemas provistos por las instituciones bancarias no se pueden considerar infalibles y, por tanto, no pueden mantener una presunción absoluta respecto a su debido funcionamiento, esto es, no se encuentran libres de riesgos en la seguridad de su operación.

Apuntó que, en ocasiones, el conocimiento de los clientes respecto de los riesgos de seguridad en línea suele ser deficiente y ello facilita los engaños y la divulgación de sus datos confidenciales que luego pueden usarse para autenticar transacciones fraudulentas.

Ante dicho escenario, la Primera Sala precisó que las instituciones financieras que participan en la banca por internet deben tener métodos confiables para autenticar a los clientes, mediante el desarrollo de sistemas eficaces para salvaguardar su información, a fin de prevenir el fraude electrónico e inhibir el robo de identidades, para lo cual, el Banco de México ha recomendado no sólo la implementación de métodos que incluyan, entre otros, el uso de contraseñas, números de identificación y certificados digitales como nivel de protección contra tales riesgos, pues el nivel de protección contra riesgos que ofrece cada una de estas técnicas varía, por lo que el Banco de México aconseja adoptar la implementación de diferentes y más novedosas técnicas como podrían ser las características biométricas de los usuarios.

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

La Primera Sala detalló que ante la presencia de los referidos riesgos, las autoridades han adecuado 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.

Dichas obligaciones, señaló la Primera Sala, 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 el marco normativo aplicable en relación con las transferencias por mecanismos electrónicos, entre ellas, las Disposiciones de carácter general aplicables a las Instituciones de Crédito, por medio de las cuales 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.

Entre otras disposiciones aplicables, la Primera Sala citó el artículo 52 de la Ley de Instituciones de Crédito, que establece que las instituciones de crédito podrán pactar la 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.

LEY DE INSTITUCIONES DE CRÉDITO

Artículo 52.- Las instituciones de crédito podrán permitir el uso de la firma electrónica avanzada o cualquier otra forma de autenticación para pactar la 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, y establecerán en los contratos respectivos las bases para determinar lo siguiente:
I. Las operaciones y servicios cuya prestación se pacte;
II. Los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y
III. 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.
[…]

La Primera Sala enfatizó que dicho reconocimiento se encuentra inmerso en los artículos 80, 89 y 94 del Código de Comercio, en los que se establece que,

para la formación de actos de comercio, pueden emplearse los medios electrónicos, ópticos o cualquier otra tecnología que se estime necesarios y se establece una serie de definiciones para explicar los mecanismos que pueden utilizarse.

CÓDIGO DE COMERCIO

Artículo 80. Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.
[…]
Artículo 89. Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.
[…]
Artículo 94. Salvo pacto en contrario entre el Emisor y el Destinatario, el Mensaje de Datos se tendrá por expedido en el lugar donde el Emisor tenga su establecimiento y por recibido en el lugar donde el Destinatario tenga el suyo. Para los fines del presente artículo:
I. Si el Emisor o el Destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal, y
II. Si el Emisor o el Destinatario no tienen establecimiento, se tendrá en cuenta su lugar de residencia habitual.

La Primera Sala subrayó de manera particular, que la Comisión Nacional Bancaria y de Valores, al emitir las Disposiciones de Carácter General aplicables a las Instituciones de Crédito,[2] estableció un capítulo específico por lo que se refiere a la operación de la banca electrónica, dentro del Título Quinto denominado "Otras disposiciones", que en el Capítulo X "Del uso del servicio de la

[2] 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, 27 de agosto, 21 de septiembre, 29 de octubre, 9 y 13 de noviembre de 2015, respectivamente.

Banca Electrónica" prevé la obligación de las instituciones de implementar mecanismos que permitan la identificación del usuario y su autenticación para poder utilizar el servicio de banca electrónica.

DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE CRÉDITO

TÍTULO QUINTO
OTRAS DISPOSICIONES
[…]
Capítulo X
Del uso del servicio de Banca Electrónica
Sección Primera
De la contratación para el uso del servicio de Banca Electrónica
Artículo 306.- Las Instituciones podrán pactar la celebración de sus operaciones y la prestación de servicios con el público, a través de servicios de Banca Electrónica, debiendo sujetarse a lo establecido por las presentes disposiciones y siempre que:
I. En la contratación respectiva se establezca de manera clara y precisa, lo siguiente:
a) Las operaciones y servicios que podrán proporcionarse a través de Medios Electrónicos.
b) Los mecanismos y procedimientos de Identificación del Usuario y Autenticación, así como las responsabilidades del Usuario y de la Institución respecto del uso del servicio de Banca Electrónica.
[…]

Después de destacar el contenido de los otros artículos que de las Disposiciones de Carácter General aplicables a las Instituciones de Crédito, relativos a la operación del servicio de banca electrónica, la Primera Sala destacó que la propia Comisión Nacional Bancaria y de Valores ha considerado que los riesgos de seguridad son un aspecto que puede llegar a afectar la situación financiera no sólo de las instituciones, sino de los usuarios mismos, por lo 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".

Precisado lo anterior, y en línea con lo que se resolvió en la referida contradicción de tesis 128/2018, la Primera Sala sostuvo que la presunción 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.

Ello, toda vez que, actualmente, se conocen diversas maneras de poder obtener de manera engañosa datos de los clientes o vulnerarse contenido electrónico para realizar operaciones fraudulentas, por lo que la institución bancaria es quien debe acreditar que los procedimientos de identificación que se utilizaron 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 se considera que el banco cuenta con la infraestructura para generar la evidencia presentada ante los órganos jurisdiccionales.

e) Decisión

La Primera Sala concluyó que no puede presumirse la fiabilidad de la banca electrónica a partir de que se acredite que se realizó una transferencia electrónica de dinero y en la cual se haya utilizado un determinado mecanismo de autenticación por parte del usuario, ya que tal presunción solamente se puede obtener una vez que la institución bancaria demuestre que se siguió el procedimiento exigido normativamente para la realización de la operación de que se trate.

Puntualizó que, cuando resulte controvertida la validez de una transacción que tenga por objeto la transferencia de dinero a cuentas de terceros u otras instituciones bancarias, no basta con acreditar que se introdujeron las claves o contraseñas para acceder al sistema electrónico, sino que la institución bancaria debe demostrar que dicha operación cumplió con el procedimiento previsto en las disposiciones aplicables, 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.

Así, la Primera Sala sostuvo que la carga probatoria es la de acreditar que el sistema dispuesto por la institución bancaria operó bajo los protocolos legalmente establecidos en el momento en que se realizó la transferencia de recursos dinerarios y que, por tanto, el sistema en sí mismo no fue vulnerado por algún agente externo.

La Primera Sala hizo énfasis en que la anterior determinación no contraviene lo dispuesto por el artículo 1196 del Código de Comercio, que establece que el que niega está obligado a probar, 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 se funde en mayores elementos probatorios para que el juez lo considere cierto y pueda aplicar esa presunción.

Precisó que lo anterior, también se sustenta en la carga de la prueba prevista en los artículos 1194, 1195 y 1196 del Código de Comercio, por medio de los cuales se impone 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 demostración de los hechos controvertidos, la cual encuentra una aplicación especial, tratándose del caso de los consumidores.

CÓDIGO DE COMERCIO

Artículo 1,194. El que afirma está obligado a probar. En consecuencia, el actor debe probar su acción y el reo sus excepciones.
Artículo 1,195. El que niega no está obligado a probar, sino en el caso en que su negación envuelva afirmación expresa de un hecho.
Artículo 1,196. También está obligado a probar el que niega, cuando al hacerlo desconoce la presunción legal que tiene a su favor el colitigante.

La Primera Sala estimó que la carga de la prueba implica que la parte que ostenta una posición dominante en la relación de consumo es la que debe acreditar el debido funcionamiento, toda vez que la tecnicidad de los sistemas digitales del servicio de la banca electrónica representaría un obstáculo excesivo para que el usuario del servicio pudiera demostrar su pretensión, a diferencia de las instituciones prestadoras del servicio de banca electrónica que se encuentran obligadas a contar con determinada infraestructura y profesionalización.

Por lo anterior, la Primera Sala determinó que las instituciones bancarias son quienes deben acreditar que el sistema de banca electrónica operó de acuerdo a la normatividad establecida al momento de llevar a cabo la operación controvertida, pues, a diferencia de los usuarios, las instituciones financieras cuentan con mayor facilidad para acceder a la información que dé cuenta de tales operaciones, en atención a la obligación de resguardo de la información, que les asiste a las Instituciones de Crédito.

Lo anterior con fundamento en el artículo 316 bis 15, de las Disposiciones de carácter General aplicables a las Instituciones de Crédito, por medio del cual se 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.

DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE CRÉDITO

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.
> […]

La Primera Sala destacó que el consumidor está en una posición de desventaja frente al prestador del servicio bancario en línea, ya que no cuenta con los mecanismos tecnológicos necesarios a los que sí puede acceder la institución bancaria, ello, aunado a 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, ya que dichos datos se encuentran bajo un resguardo riguroso al que no puede tener acceso cualquier persona.

De esta manera, la Primera Sala hizo notar que a fin de dilucidar ese tipo de controversias los jueces necesitan una evaluación integral respecto de quién efectuó la transacción, 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 quien efectuó las transacciones, o en todo caso, perdió el deber de cuidado que debe tener sobre su información personal.

En ese sentido, la Primera Sala enmarcó que 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*.

Por ende, la Primera Sala reiteró que 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 es suficiente para acreditar la validez de la transacción y, de ser el caso de que la institución bancaria tuviere conocimiento de cualquier incidente que pudiera haber comprometido los datos del cuentahabiente, debe declararlo.

Asimismo, consideró que una vez acreditado que el procedimiento normativamente exigido de la institución financiera para la operación impugnada se siguió debidamente y que además, no se tuvo conocimiento de incidentes que comprometieran los datos del cuentahabiente, no se le puede exigir a la institución financiera la carga de demostrar la fiabilidad del sistema, la cual se presumirá 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 de que no existió ningún tipo de vulneración.

Enfatizó que no puede llegarse al extremo de exigirle a la institución financiera que demuestre la fiabilidad 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 de 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 le corresponde 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 las 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.

La Primera Sala estableció que dicha carga no se considera excesiva para las instituciones del sector financiero, dado que encuentra su justificación en la protección reforzada que asiste a los consumidores, pues 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, no limita la protección que deba asistirles.

Sobre este aspecto, resaltó que los servicios financieros encuadran en una relación de consumo en la cual los usuarios del servicio tienen la calidad de consumidores y las instituciones bancarias la calidad de proveedoras del servicio y, si bien la protección de los usuarios encuentra su cauce en una legislación especial, éstos no pierden su calidad de consumidores, ni la protección que les asiste en términos del artículo 28 de la Constitución General, 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.

Finalmente, con base en tales consideraciones, la Primera Sala determinó que debe prevalecer con carácter de jurisprudencia el siguiente criterio:

"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."[3]

El criterio contenido en la tesis anterior se aprobó por unanimidad de cinco votos de las señoras **Ministras** y los señores **Ministros Jorge Mario Pardo Rebolledo** (Ponente), **Norma Lucía Piña Hernández, Ana Margarita Ríos Farjat** (Presidenta), **Juan Luis González Alcántara Carrancá** y **Alfredo Gutiérrez Ortiz Mena**.

[3] Tesis: 1a./J. 17/2021 (10a.), *Gaceta del Semanario Judicial de la Federación*, Undécima Época, Libro 1, Tomo II, mayo de 2021, página 1752, registro digital: 2023157.