CONTRADICCIÓN DE TESIS 128/2018.
ENTRE LOS CRITERIOS SUSTENTADOS POR EL TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO Y EL SEGUNDO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL SEXTO 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, correspondiente al día **nueve de enero de dos mil diecinueve.**

V I S T O S; y,

R E S U L T A N D O:

PRIMERO. Denuncia de la Contradicción. Mediante oficio I-64/2018, presentado el nueve de abril de dos mil dieciocho, ante la Oficina de Certificación Judicial y Correspondencia de esta Suprema Corte de Justicia de la Nación, los Magistrados integrantes del **Segundo Tribunal Colegiado en Materia Civil del Sexto Circuito**, denunciaron la posible contradicción de tesis entre el criterio emitido por dicho órgano colegiado al resolver el juicio de amparo directo **402/2017**; y el criterio sustentado por el **Tercer Tribunal Colegiado en Materia Civil del Primer Circuito**, al resolver el juicio de amparo directo **499/2016.**

SEGUNDO. Trámite de la denuncia. Mediante acuerdo de dieciséis de abril de dos mil dieciocho, el Presidente de la Suprema Corte

de Justicia de la Nación admitió a trámite la denuncia de la contradicción de tesis, ordenó formar y registrar el expediente bajo el número 128/2018.

En el mismo proveído se solicitó a las Presidencias de los tribunales colegiados contendientes remitir, por conducto del MINTERSCJN, la versión digitalizada de la ejecutoria contendiente de su índice. Por otra parte, se pidió al **Tercer Tribunal Colegiado en Materia Civil del Primer Circuito** remitiera la versión digital del proveído que informe si el criterio sustentado en su ejecutoria contendiente se encuentra vigente o, en su caso, la causa para tenerlo por superado o abandonado. Por último, se ordenó remitir los autos para su estudio a la ponencia del señor Ministro Jorge Mario Pardo Rebolledo.

TERCERO. Integración del asunto en la Primera Sala y avocamiento. En cumplimiento al proveído de admisión, por acuerdo de dos de mayo de dos mil dieciocho, dictado por la Presidenta de la Primera Sala de la Suprema Corte de Justicia de la Nación, se tuvieron por recibidos los autos de la contradicción de tesis número 128/2018.

En el mismo proveído se ordenó el avocamiento del asunto en la Primera Sala, mandando se enviaran los autos -una vez integrados- a la ponencia del señor Ministro Jorge Mario Pardo Rebolledo, para la elaboración del proyecto de resolución. Asimismo, se solicitó vía MINTERSCJN a los tribunales colegiados contendientes, para que informaran si sus respectivas sentencias ya habían causado ejecutoria.

En diverso auto de fecha cuatro de mayo de dos mil dieciocho, dictado por la Ministra Presidenta de esta Primera Sala, se hizo constar que los tribunales contendientes remitieron copia digitalizada

de sus sentencias; en el mismo auto se tuvo al **Tercer Tribunal Colegiado en Materia Civil del Primer Circuito** informando que no se ha apartado del criterio sustentado en su sentencia contendiente.

Mediante proveído de diez de mayo de dos mil dieciocho, se tuvo a los tribunales colegiados contendientes informando que su sentencia contendiente ha causado ejecutoria, por lo que al estar debidamente integrado el expediente, se enviaron los autos a la Ponencia del 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, atendiendo a lo dispuesto en los artículos 107, fracción XIII, de la Carta Magna; 226, fracción II de la Ley de Amparo vigente; en relación con los puntos primero, segundo y tercero del Acuerdo General 5/2013, emitido por el Pleno de este Alto Tribunal y publicado en el Diario Oficial de la Federación, el veintiuno de mayo de dos mil trece; en virtud de que se trata de una posible contradicción de tesis entre Tribunales Colegiados de diversos Circuitos, y el tema de fondo corresponde a la materia civil, en la que se encuentra especializada esta Sala.

SEGUNDO. Legitimación. La denuncia de contradicción de tesis proviene de parte legítima, 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, pues fue realizada por los Magistrados integrantes del Segundo Tribunal Colegiado en

Materia Civil del Sexto Circuito, el cual es uno de los órganos entre los que se suscita la posible contradicción, por lo que se actualiza el supuesto de legitimación a que aluden los referidos preceptos.

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. Tercer Tribunal Colegiado en Materia Civil del Primer Circuito, quien conoció del **juicio de amparo directo 499/2016**, del cual se advierten los antecedentes siguientes:

Juicio oral mercantil. Graciana Vázquez Sánchez demandó de BBVA Bancomer, Sociedad Anónima, Institución de Banca Múltiple, Grupo Financiero BBVA Bancomer (en lo subsecuente “el Banco”), las siguientes prestaciones: **a)** la nulidad de *siete pagarés*, los cuales fueron emitidos al amparo de una tarjeta de crédito cuya titular era la actora; **b)** el pago de $******* (******* *******), cantidad que corresponde al total de los cargos efectuados a la mencionada tarjeta; **c)** el pago de los intereses legales generados por la cantidad referida; y **d)** el pago de gastos y costas.

Del asunto conoció la Jueza Octavo de Distrito en Materia Civil en la Ciudad de México, bajo el número *******. Seguida la secuela procesal, el treinta y uno de mayo de dos mil dieciséis, la jueza referida dictó sentencia en la que declaró la nulidad de los vouchers que dieron origen a los cargos provenientes de la tarjeta de débito, por lo cual condenó a la demandada al pago de la cantidad reclamada y de los intereses legales; sin embargo no se hizo condena en costas.

Juicio de amparo directo. En contra de dicha resolución, el Banco promovió juicio de amparo del cual conoció el Tercer Tribunal Colegiado en Materia Civil del Primer Circuito, bajo el número 499/2016, quien dictó sentencia el diez de agosto de dos mil dieciséis, en el sentido de conceder el amparo para el efecto de que la responsable dejara insubsistente la sentencia reclamada y, en su lugar, dictara otra en la que se desacreditara la nulidad de dos pagarés, pues el Banco demostró que los mismos se realizaron mediante la utilización de la firma electrónica de la actora.

Dicha determinación la sustentó -en lo que interesa para la resolución de la presente contradicción-, en los razonamientos siguientes:

> Resultó fundado el argumento de la quejosa en el que adujo que no fueron debidamente analizadas la totalidad de las pruebas ofrecidas, y que esa circunstancia motivó que en la sentencia reclamada se emitieran razonamientos contradictorios con los autos.
>
> Lo anterior, puesto que del escrito de contestación a la demanda advirtió que el banco aceptó haber realizado los cargos reclamados, a través de medios electrónicos, mediante el uso de la firma electrónica de la actora, lo cual trajo como consecuencia, la emisión de los folios de autorización correspondientes.
>
> En la misma línea, se resalta que el banco ofreció copia certificada de los vouchers derivados de consumos efectuados en Office Depot de México, Sociedad Anónima de Capital Variable por un monto de $******* (*******) y Bisutería Barrios, por un monto de $******* (*******).
>
> También refiere que, para el banco, tales documentos son suficientes para liberarla de responsabilidad, por el uso y custodia de la firma electrónica, la cual es de exclusiva salvaguarda del cliente, conforme a la cláusula décima sexta del contrato, lo que permite identificarlo plenamente.
>
> Con base en ello, el tribunal colegiado destacó que, de manera voluntaria, el banco emisor asumió la carga probatoria de la validez de los cargos realizados, en tanto que arrojó al

tarjetahabiente, la carga de probar que las operaciones se hicieron a través de una mecánica distinta a la prevista contractualmente, es decir, sin la utilización de la firma electrónica o mediante ésta, por persona distinta al cliente, sin su autorización y que dio aviso a la demandada del robo, pérdida, extravío o mal uso de cualquiera de los dispositivos de seguridad, incluyendo la firma electrónica.

Por tanto, como se adelantó, el tribunal colegiado calificó de fundado el argumento ya que al exhibir copia certificada de los documentos que respaldaron las compras efectuadas mediante firma electrónica se debió tener por cumplido el requerimiento efectuado al banco por el Juez responsable, pues se debió considerar que al tratarse de transacciones realizadas mediante firma electrónica, la exhibición de éstas en copia certificada daba cumplimiento a su obligación de conservar los documentos que respalden las compras efectuadas por sus clientes a través de una tarjeta de crédito o débito, de conformidad con los artículos 99, 100 y 115, de la Ley de Instituciones de Crédito y con las *"Reglas a las que habrán de sujetarse las instituciones de banca múltiple en la emisión y operación de tarjetas de crédito bancarias",* emitidas por el Banco de México, pues de conformidad con dicha legislación las entidades bancarias o crediticias están facultadas para microfilmar o grabar en discos ópticos o en cualquier otro medio que autorice la Comisión Nacional Bancaria y de Valores, libros, registros y documentos en general que obren en su poder.

Por lo que, el banco al haber cumplido con su carga procesal de exhibir los referidos vouchers cuestionados y proceder a su análisis, se debió advertir que contienen las leyendas *“autorizado mediante firma electrónica”* y “*pin verified*”, los folios de autorización que les sucedieron a dichas transacciones, así como la constancia del día y la hora en que fue utilizada estrictamente por el cliente.

Derivado del error identificado, el tribunal colegiado procedió a analizar la naturaleza de las compras efectuadas mediante firma electrónica.

En primer lugar, refirió que la firma electrónica es el conjunto de datos, en forma electrónica, anexos a otros datos electrónicos o asociados funcionalmente a ellos, utilizados como medio para identificar formalmente al autor o los autores del documento que la recoge.

Después, transcribió el artículo 89 del Código de Comercio, así como el artículo 2° de las reglas de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, pues en ambos preceptos se define a la firma electrónica.

Refirió que la Ley Modelo mencionada, en los artículos 6 y 7, establece que los requisitos que deben ser cumplidos para la firma electrónica se tendrán como válidos, como expresión del consentimiento válidamente prestado, con un mensaje de datos.

También señaló que la Guía para la incorporación de la Ley Modelo en comento plasma la función de la firma electrónica.

De las referencias a los instrumentos mencionados obtuvo que, el uso de la firma electrónica en las operaciones bancarias constituye una fuente válida de obligaciones para los tarjetahabientes que se vinculan a dicho mecanismo de seguridad para las transacciones comerciales.

Por lo que tales reglas, surgen para estandarizar los actos de comercio por medios electrónicos a fin de dotarlos de contenido obligacional.

Destacó que si bien la firma autógrafa es el medio por excelencia para crear el vínculo entre las partes que intervienen en la creación de un acto jurídico, lo cierto es que los medios electrónicos han permitido realizar operaciones comerciales entre personas que se encuentran en distintos lugares; sin embargo, se ha cuestionado si la información trasmitida mediante datos electrónicos es suficiente para construir el acto jurídico y dotarlo de validez, por ello es que la ley modelo referida establece las reglas para crear una firma electrónica que al ser utilizada vincule a quien la emite.

Así, la ley modelo en comento establece como eje rector de la firma electrónica la fiabilidad en su creación; lo cual otorgará certeza a quien la posee que sólo éste puede utilizarla y, por ende, es fuente de obligaciones.

Por tanto, una vez acreditado el método de creación de la firma electrónica, su ingreso al sistema de datos genera un vínculo jurídico que torna en incuestionable si fue el titular quien utilizó la firma electrónica; siendo que sólo podrá ponerse en duda la fiabilidad del método de creación.

A pesar de la información obtenida de las leyes modelo, señaló que ésta debe ser analizada en concatenación con lo dispuesto por el artículo 97 del Código de Comercio.

Después del marco referencial en torno a la firma electrónica, el tribunal colegiado señaló que en los dos vouchers arriba mencionados, se encontraban insertos los siguientes datos:

1. Los últimos cuatro dígitos del número de tarjeta de débito.
2. El número de cada operación.
3. Fechas en que se realizaron los cargos.
4. Hora en que se realizaron los cargos.
5. Nombre de la negociación que realizó el cargo a la tarjeta de crédito.
6. La leyenda "*Pin Verified"* y "*Autorizado mediante firma electrónica"*.
7. El folio de aprobación o autorización del cargo que le precedió.

Por tanto, si los vouchers contenían tales datos, entonces el juzgador responsable -para efectuar una correcta valoración de dichos medios de convicción y determinar el cumplimiento de las cargas probatorias de las partes del juicio-, debió analizar en primer lugar que las operaciones bancarias se realizaron mediante el uso de la tarjeta de débito y el ingreso de la firma electrónica, conocida como número de identificación personal, y por sus siglas en inglés PIN.

Máxime que, las normas sobre firmas electrónicas califican de válido los actos jurídicos donde se ingrese este tipo de firmas sin cuestionar la fiabilidad del método de uso, sino sólo el de creación, por tanto la institución bancaria ante una acción de nulidad por desconocimiento de la transacción comercial sólo debe acreditar que se realizaron electrónicamente las operaciones que generaron los cargos por cualquier medio de prueba y 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.

En ese sentido, la parte que cuestiona la certeza de la transacción tenía la carga de acreditar que no se utilizó en dicha transacción la tarjeta ni el PIN personal con los que se realizó la operación bancaria, y no solo desconocer las reglas del comercio electrónico.

Para reforzar tal conclusión, el tribunal colegiado distinguió entre la fiabilidad de la firma electrónica y la certeza de la operación bancaria como fuente de obligaciones.

En cuanto a la fiabilidad de la firma electrónica resaltó que el artículo 6 de la ley modelo, acogido por el artículo 97 del Código de Comercio, señalan los requisitos que debe contener la creación de una firma electrónica para considerarla fiable, en otras palabras, señalan los datos que se integran a un archivo electrónico que generara un criptograma y que servirá para activar el password o PIN que constituirá la firma electrónica.

Respecto la certeza de la operación, señaló que sus elementos materiales, es decir, la seguridad en que quien realizó la operación es el titular de la firma electrónica; no encuentran sustento en su ámbito personal, pues no equivale a la firma autógrafa, sino en la utilización del password o PIN, ya que los medios electrónicos que se utilizan como la terminal punto de venta (TPV) y el sistema operativo que traduce la información, derivan de fuentes internacionalmente aceptadas y, por ende, su cuestionamiento compete a quien lo pone en tela de juicio bajo el principio ontológico de la carga de la prueba, según el cual lo ordinario se presume y lo extraordinario se prueba, siendo lo ordinario que las TPV y el sistema operativo no sean vulnerables, por ende, corresponde la carga de la prueba a quien alega lo contrario.

De allí que los elementos de seguridad en este tipo de operaciones no están compuestos por la fecha y hora de la operación, ni el análisis de su fiabilidad mediante la prueba pericial; sino porque existe fiabilidad en su proceso de creación y los sistemas utilizados son estandarizados para realizar las operaciones comerciales mediante el uso de la firma electrónica.

Bajo tales razonamientos, apuntó que la firma electrónica resulta fiable y es fuente de obligaciones, cuando satisface los requisitos para su creación a menos que se demuestre que su proceso de creación la hace vulnerable.

Pero, desde el punto de vista operativo la operación debe ofrecer los datos que permiten al usuario y a la banca saber que se realizó la operación mediante el uso de la firma electrónica. Por ello, como las citadas normas persiguen dotar de efectos jurídicos cualquier método de creación de una firma electrónica, es

consecuencia que el uso de la firma electrónica resulte una fuente válida de obligaciones para las partes.

También refirió que en México se obligó a sustituir el uso de banda magnética y la firma autógrafa, por el CHIP y la firma electrónica a partir del año dos mil trece. Siendo que la ventaja de tal firma es que sólo el usurario la conoce y no queda constancia de ella en las operaciones que realiza; sólo un registro que se autorizó la operación al haberse ingresado la firma electrónica.

Abundó en el tema señalando que el uso de la tarjeta bancaria mediante la firma electrónica supone el uso de un *"chip"*, que es un elemento de seguridad encriptado que se vincula al *password* o número de identificación personal y del que sólo podría mirarse, en caso de acceder, su criptografía, pero nunca se podría saber que pertenece al usuario porque se trata de una mera secuencia de números y/o letras que precisamente por seguridad se desconoce su conformación, en la que interviene el sistema operativo que las crea.

Así, no podría existir prueba sobre estos elementos, porque el acceso a las operaciones bancarias de manera directa no arrojaría algún dato, en tanto su contenido o criptografía, simplemente resultaría inteligible, porque el password o PIN sólo lo conoce el cliente y se encuentra desvinculado del CHIP.

Con base en todas las premisas reseñadas, recalcó que si el uso de la tarjeta de crédito descansa en un contrato en el que el tarjetahabiente asumió el uso de la firma electrónica como fuente de obligaciones, que sólo él conoce y que lo único que está a discusión es si el tarjetahabiente efectuó la operación, entonces la distribución de la carga de la prueba debe regirse por lo dicho en los párrafos precedentes.

En cuanto a la carga probatoria, señaló que son varios los principios que rigen la carga de la prueba y que actualmente se orientan por la doctrina de la dinámica probatoria; sin embargo, que tal doctrina no soslaya el principio lógico, sino que en función de los hechos expuestos por las partes y del conocimiento de su actividad, se redistribuye la carga de la prueba.

También señaló que las normas sustantivas suelen regular a quién corresponde la carga de la prueba, por lo que la existencia de una disposición expresa deja fuera toda posibilidad de distribuir la carga de la prueba de una manera distinta a la prevista en la

> norma; a menos que previamente se realice una examen de convencionalidad.

Pues bien, nuevamente regresa al estudio del caso concreto, y refirió que el artículo 96 del Código de Comercio parte de la base que el uso de la firma electrónica es fuente de obligaciones sin perjuicio de que pueda desvirtuarse su fiabilidad; de ahí que, a quien corresponde la carga de la prueba para desvirtuar la fiabilidad de la firma es a quien la cuestiona; siendo que en el caso le corresponde a la actora, pues el cargo genera la presunción legal, conforme a este precepto, del consentimiento en la operación.

De allí que el banco no estaba obligado a demostrar que la operación es fiable, sino que la operación se realizó con el consentimiento de la tarjetahabiente, lo que se acreditó con el cargo a su tarjeta mediante el uso de la firma electrónica.

Por tanto, a partir de los medios de prueba referidos se construyó una prueba plena respecto que la operación bancaria se realizó con consentimiento de la actora en cuanto a los cargos efectuados por los establecimientos Office Depot de México, Sociedad Anónima de Capital Variable y Bisutería Barrios.

Derivado de todo lo anterior, determinó que los vouchers en estudio cumplieron con los requisitos establecidos en el artículo 170 de la Ley General de Títulos y Operaciones de Crédito, por lo que fue incorrecto que se condenara a la quejosa al pago de las cantidades cobradas con motivo de dichas transacciones.

No pasó desadvertido que los referidos vouchers contienen una firma gráfica de cuyos rasgos no se advierte correspondencia con la firma de la actora; sin embargo, en las transacciones autorizadas mediante firma electrónica, la transacción no es autorizada por virtud de la firma estampada sino por virtud de la firma electrónica y ante ello, la diversidad de las firmas pasan a un segundo término por no ser el medio de autorización de dicha transacción.

II. Criterio del Segundo Tribunal Colegiado en Materia Civil del Sexto Circuito, quien conoció del **amparo directo 402/2017**, del que se desprenden los antecedentes siguientes:

Juicio oral mercantil. Erasmo Álvarez Méndez demandó de BBVA Bancomer, las siguientes prestaciones: **a)** la declaración de nulidad de *un pagaré*, el cual fue emitido al amparo de una tarjeta de débito cuyo titular fue el actor; **b)** la declaración judicial de que la citada operación se realizó sin su consentimiento y autorización; **c)** la devolución de los fondos dispuestos, consistente en la cantidad $******* (*******); **d)** el pago de intereses; **e)** y el pago de gastos y costas.

Del asunto conoció el Juez Primero de Distrito en Materia de Mercantil, Especializado en Juicios de Cuantía Menor con residencia en San Andrés Cholula, Puebla, bajo el número de expediente *******, mismo que fue resuelto el cuatro de julio de dos mil diecisiete, en el sentido de declarar la nulidad del voucher y condenar a la demandada al pago de la cantidad referida y de los gastos.

Juicio de amparo. En contra dicha resolución, la parte demandada promovió juicio de amparo, del cual conoció el Segundo Tribunal Colegiado en Materia Civil del Sexto Circuito bajo el número 402/2017, mismo que fue resuelto en sesión de uno de marzo de dos mil dieciocho, en el sentido de negar el amparo.

La argumentación esgrimida por el órgano contendiente en la presente contradicción de tesis, es la siguiente:

> Resultaron infundados los conceptos de violación en torno a que el juez responsable determinó erróneamente la carga de la prueba.
>
> Resaltó que el juez responsable determinó tal carga para el banco como la obligación de justificar la adopción de todas aquellas medidas de seguridad que condujeran a la conclusión de que los sistemas electrónicos a través de los cuales sus clientes realizan actos de comercio mediante la utilización de la tarjeta bancaria

> que les proporciona y la firma electrónica o NIP, tengan el menor grado de falibilidad posible, y que razonablemente conduzca a establecer su certeza.

También refiere que, en contra de tal determinación, la quejosa adujo que deben tomarse en cuenta las reglas generales en materia probatoria contenidas en el Código de Comercio.

Partiendo de lo resuelto y lo hecho valer por la quejosa, el tribunal colegiado determinó que en el caso concreto, este es, cuando se impugna una operación comercial realizada mediante una tarjeta bancaria, en la cual se utilizó como medio de convalidación una firma electrónica, no puede resolverse con base en las reglas generales en materia probatoria previstas en el Código de Comercio, pues en caso de seguirlas, ello conduciría a un escenario en que la carga procesal sería prácticamente de imposible cumplimiento para aquél que pretende la nulidad de tal operación.

Explica detalladamente el asunto que se sometió a su consideración, el cual tiene las siguientes particularidades: la operación impugnada de nula se llevó a cabo en la realidad -lícita o ilícitamente-, la cual para su verificación, se utilizó la información contenida en la banda magnética o microchip asociado a la tarjeta entregada al cliente de una institución bancaria, conjuntamente con la digitación de la firma electrónica del cuentahabiente -conocida como número de identificación personal o NIP-, en el lector electrónico otorgado por una institución bancaria a un tercero, denominada terminal punto de venta.

Refirió que tal información es la necesaria para llevar a cabo las operaciones de comercio electrónico en dicha modalidad, siendo que la custodia, resguardo y buen uso tanto del plástico como del NIP, son responsabilidad del cliente o cuentahabiente.

Pues bien, considera que el asunto arroja dos escenarios: el primero, consistente en que toda operación de comercio electrónico realizada con la utilización de la información contenida en la banda magnética o microchip de una tarjeta y con la digitación del NIP o firma electrónica asociado a ella, deba ser considerada incontrovertiblemente válida, es decir, llevada a cabo indefectiblemente por el cliente; o, el segundo, relativo a la posibilidad de impugnar esa operación, bien sea por que esos elementos se hubieran utilizados ilícitamente, esto es, con motivo

de su indebida duplicidad, o por haber sido robados u obtenidos violentamente.

Sin embargo, derivado de los autos consideró que en el caso concreto ocurrió una duplicidad indebida de la citada información, conocida comúnmente como clonación.

Así, reconoció que en el caso de clonación no resulta fácil establecer a quién corresponde la carga probatoria, pues para ello, primero debe identificarse qué es lo que sería posible de ser justificado, ya que de lo contrario se asignarían obligaciones de difícil o incluso de imposible cumplimiento.

En ese sentido, el problema consiste en determinar si el actor que pretende la nulidad de la operación tiene la carga de demostrar:

i. La forma en cómo fue duplicada indebidamente o clonada su información bancaria;
ii. La falibilidad o vulnerabilidad de los medios de almacenamiento electrónico en que se resguarda la identidad de los señalados mecanismos electrónicos o cibernéticos; o,
iii. La falta de fiabilidad o seguridad del medio de creación de la firma electrónica o número de identificación personal de un usuario de servicios de banca electrónica.

O bien, si corresponde por carga probatoria al banco demandado demostrar:

i. La autenticidad de la operación, por haberse utilizado en ella la tarjeta única u original otorgada al cuentahabiente y, en su caso, con la digitación por él de su firma electrónica;
ii. La confiabilidad del medio de resguardo y almacenamiento de la información del cliente o cuentahabiente, que constituyen su identidad electrónica;
iii. La seguridad del medio de creación de la información que permite la identificación de un usuario de alguno de los mecanismos de comercio electrónico existentes, es decir, de su firma electrónica o NIP.

A partir de la identificación de los distintos extremos que podrían considerarse al momento de hacer la asignación o distribución de las cargas probatorias, concluyó que no pueden tomarse en cuenta solo las reglas generales contenidas en el Código de Comercio -las cuales fueron emitidas antes de la existencia de las operaciones de comercio electrónico-, sino también las relativas

a la posibilidad o menor dificultad para justificar los citados elementos, ponderando en dicho evento la especial condición de cada una de las partes, así como la forma en que se relacionan al contratar y realizar operaciones de banca electrónica, y en función de ello la mayor o menor posibilidad de justificar el hecho materia de discusión.

Así, la clonación de información electrónica significa, por un lado, la obtención indebida, es decir, sin autorización de quienes podrían otorgarla, y mediante la utilización de desarrollos tecnológicos, aportados por la ciencia, en concreto por la cibernética, de la identidad digital de un usuario de los servicios de banca electrónica; y por el otro, la utilización de esa información, que es idéntica a la original, mediante la suplantación del titular de esa información de la identidad digital robada o ilícitamente alcanzada, al momento de llevar a cabo una operación comercial.

Por lo que si la clonación consiste en la duplicación de datos o información electrónica que no debería ser replicada, a nada práctico conduciría atribuir a la persona que se dice víctima, la obligación de demostrar tal evento, es decir, que los elementos que permitirían identificarlo electrónicamente, tanto con una cuenta bancaria, a partir de la información contenida en la cinta magnética o microchip incorporado a una tarjeta de debido o de crédito, como con el número de identificación asociado a ella, fueron idénticamente reproducidos, pues la conclusión sería la misma, es decir, que la operación electrónica objetada se llevó a cabo mediante la utilización de la información que el banco otorga a sus clientes, al momento en que les entrega sus respectivas tarjetas y se genera la firma electrónica correspondiente; y que por tal motivo deben responder por los cargos efectuados objeto de impugnación. Dicha forma de razonar anula por completo la posibilidad de éxito de la acción al alcance de los cuentahabientes de oponerse a las operaciones ilícitas realizadas en su perjuicio, trasladándoles así el costo económico derivado de la facilidad tecnológica existente para duplicar o clonar la identidad electrónica de los usuarios de la banca.

Pero el problema se circunscribe en que esa información, la cual es confidencial, no se vuelva vulnerable. Y si lo es, que se adopten todas aquellas medidas que permitan evitar su indebida o ilícita utilización.

Recordó que esto último es en lo que puso énfasis el juez responsable, respecto de lo cual coincide.

Precisó que en los casos en que para la realización de una actividad de comercio electrónico se emplea una terminal, en la cual se introduce o desliza una tarjeta bancaria y se digita en el teclado el número de identificación personal o firma electrónica, la certeza y legalidad se da porque el titular de la cuenta bancaria fue el que hizo uso de la tarjeta y del NIP asociado a ella, y no únicamente por la presencia del plástico que contenga la citada información y de la ejecución del mencionado NIP.

Al respecto resaltó que, dichos aparatos o mecanismos son manipulados por seres humanos, de manera tal que el receptor del citado medio electrónico de pago, como sana práctica mercantil, y por seguridad tanto de la operación como de quienes en ella intervienen (usuario de la tarjeta, vendedor o proveedor de servicios que recibe el pago y la o las instituciones bancarias en que se encuentran aperturadas las cuentas en las que se realizan los respectivos movimientos activo y pasivo) debe constatar la identidad de quien pretende hacer uso de la tarjeta, **por lo que razonablemente se le puede exigir que, como condición para aceptar el citado mecanismo de pago, solicite algún documento oficial que sirva como identificación de quien lo utiliza o pretende utilizarlo, a efecto de corroborar que se trate del titular de la cuenta asociada a la respectiva tarjeta bancaria** (para el evento de que su nombre aparezca grabado en ella o, en su caso, se imprima en el voucher o pagaré que emite la terminal o en última instancia, deje constancia de quién es la persona en cuestión, en caso de que ninguno de esos datos pueda obtenerse de la tarjeta o del voucher que ampare la operación realizado), pudiendo consignarse el nombre o forma de identificar a la persona que utiliza la tarjeta bancaria que sirve como medio electrónico de pago, a fin de corroborar de la legitimación del usuario que interviene en el acto de comercio.

Consideró que en lo anterior debe ponerse atención, pues al resultar razonable la referida obligación a quien celebra una operación de comercio electrónico, entonces se puede establecer la distribución de cargas probatorias, ya que debe de constatar la identidad de la persona que al amparo de una tarjeta bancaria pretende celebrar un acto mercantil, como forma o mecanismo que conduzca a la certeza del acto cuestionado. Y como las instituciones bancarias son las que cuentan con los recursos humanos y tecnológicos o de cualquier otra índole a su alcance para arribar a dicho escenario, entonces al Banco demandado le corresponde la carga probatoria. Apunta que esto fue resuelto por la autoridad responsable, con lo cual concuerda.

Al respecto, abundó señalando que la institución bancaria demandada participó de manera indirecta en la realización de la operación de comercio electrónico, pues a través de las conexiones electrónicas que se han desarrollado efectuó el cargo respectivo en los fondos de la cuenta bancaria del actor. **Y como institución proveedora del mencionado servicio de banca electrónica, tiene el deber de adoptar todas aquellas medidas que doten de seguridad a sus clientes tanto en las operaciones que celebren, como para evitar aquellas que en su nombre y contra su patrimonio se pretendan realizar ilícitamente.**

Aterrizó tal idea en el caso concreto, y señaló que el voucher o pagaré no contiene algún dato que permita establecer la identidad de la persona titular de la cuenta bancaria, sino solamente aparece el número de tarjeta utilizada y una leyenda que dice *"Nip Verificada"*. Ello, le permitió apreciar los alcances del juez responsable en torno a la distribución de las cargas probatorias, la cual le fue atribuida al banco demandado, pues como operador de los sistemas cibernéticos con que se llevan a cabo las operaciones de comercio electrónico, tiene la obligación de justificar la adopción de todas aquellas medidas de seguridad que den certeza de la operación realizada, es decir, de que fue llevada a cabo por el titular de la cuenta bancaria contra la que se efectúa el cargo cuestionado.

En otras palabras, el banco demandado, como operador del sistema electrónico del pago, puede diseñar un sistema que permita conocer la identidad de la persona portadora de una tarjeta bancaria, que es utilizada en una terminal, tan solo con permitir que su nombre aparezca visible en la impresión del comprobante de esa operación, conocido como voucher o pagaré, y esto último, es lo que haría posible que la persona que opera la mencionada terminal, esté en condiciones de solicitar a quién le entrega la tarjeta, su identificación para constatar que se trate del titular de la cuenta o de persona autorizada en ella por este. De lo contrario, estaría facultado para rechazar la operación pretendida (o celebrarla bajo su riesgo), pero no a cuenta de quien no es titular del derecho bancario para hacer uso lícito de una tarjeta y de la firma asociada a ella, es decir, para disponer de los recursos depositados en una cuenta bancaria o de una línea de crédito a disposición del cliente o cuentahabiente.

Sentado lo anterior, vislumbra que en caso contrario, este es, que se arroje la carga de la prueba al cliente o acreditado, se le

atribuiría una obligación de difícil o incluso imposible cumplimiento, pues para ello tendría que demostrar la existencia de la duplicación indebida de su identidad electrónica a efecto de acreditar, de manera refleja o indiciaria su ilícita utilización. Es decir, el actor tendría por obligación procesal identificar o localizar por sí o con intervención de auxiliares, el sistema electrónico o cibernético con capacidades tecnológicas para llevar a cabo la clonación de una tarjeta bancaria, y el mecanismo o artilugio a través del cual se podría obtener la firma electrónica o NIP asociado a ella, para finalmente, demostrar indirectamente la factibilidad de que hubiera sido utilizado por persona distinta a él.

Con base en todas las consideraciones anteriores, concluyó que en cuanto a la certeza de una operación de comercio electrónico, es la autenticidad en cuanto a la lícita utilización de los elementos necesarios para ello, lo cual finalmente descansa en la expresión de la voluntad de la persona con capacidad jurídica para ello, es decir, en el consentimiento de aquél a quien se reputa autor o participante en el acto jurídico.

Y tal aspecto -la concurrencia de la voluntad del titular de la cuenta contra la que se hace el cargo amparado por una operación de comercio electrónico- es susceptible de ser demostrado en un procedimiento, correspondiéndole la carga probatoria de la operación a la institución bancaria y tiene por materia la justificación de todas aquellas medidas adoptadas que razonablemente puedan conducir a establecer la seguridad del mecanismo empleado, es decir, en cuanto a la seguridad de que la persona que utiliza la tarjeta bancaria como medio de pago, es el titular de la misma.

Recalcó que, aun cuando se rindiera prueba pericial ofrecida por el cliente de una institución bancaria, cuya finalidad fuera establecer cuál habría sido la firma electrónica utilizada en una operación de comercio electrónico cuya realización el cuentahabiente no reconoce como propia, ello a nada práctico conduciría, pues el resultado de la prueba sería previsible: *La operación se validó mediante la digitación de los caracteres que constituyen la firma digital o NIP correctos, es decir, que no fue autorizada dicha operación con un número distinto, y que la falla del sistema no radica en dicho aspecto*; sin embargo, el problema no estriba en establecer la existencia de una firma electrónica que se hubiera aceptado como válida sin serlo, sino en que los señalados elementos, habrían sido utilizados por una persona sin facultades para ello, y que ante tal evento no se hayan tomado medidas necesarias y razonables para evitarlo; o visto desde su

aspecto positivo, para corroborar la identidad de la persona que utiliza la información contenida en la banda magnética o microchip de una tarjeta y la firma electrónica asociada a ella, con la persona que aparece como titular en la tarjeta misma, en el voucher, o que de alguna manera permitiera lograr su identificación al momento en que se acepta su voluntad como elemento de existencia y su consentimiento válido en la realización de una operación de comercio digital, cibernético o electrónico, cuando los citados elementos son utilizados a través de una terminal otorgada por alguna institución bancaria a un comerciante o persona física o moral que pretende recibir pagos por productos o servicios que expende o brinda.

En respuesta a diversos conceptos de violación, apuntó que la causa de la nulidad radica en la ausencia de la voluntad del autor del acto, y no en la incorrección del medio de creación o validación de la firma electrónica utilizada. Por lo cual, no existen razones suficientes para establecer que debiera corresponder al cliente la obligación procesal de justificar la falibilidad del medio de creación de la firma electrónica que se encuentra asociada a la tarjeta bancaria con que realiza sus operaciones de pago, como modalidad contractualmente pactada con dicha institución; mucho menos alguna irregularidad en los elementos o caracteres de la firma electrónica en cuestión.

Por otra parte, aclaró que no es materia de estudio los elementos de lo que se denomina *"Firma Electrónica Avanzada"* o *"Firma Electrónica Fiable"*, regulada en el artículo 97 del Código de Comercio, cuyos elementos constitutivos, de creación, validación y constatación en cuanto a su existencia y corrección, son distintos de los que se utilizan al momento en que se genera un número de identificación personal o NIP que se asocia a una tarjeta bancaria.

Con base en ello, desestimó los argumentos hechos valer por la quejosa referentes a que la obligación procesal que podría asistir al cliente en el procedimiento mercantil de origen, de justificar la falibilidad del medio de generación de la firma electrónica que se utilizó en la operación cuestionada, **pues en ella no se utilizó una "*Firma Electrónica Avanzada*" y dichas alegaciones tiene apoyo en los requisitos y condiciones que aplican a las mencionadas firmas avanzadas o fiables.**

Por último, precisó que tampoco puede aceptarse la postura de la quejosa en cuanto a que para demostrar el tercero de los

> elementos de la acción de nulidad ejercida, y haciendo un ejercicio de analogía o similitud entre el evento analizado en el juicio natural con la diversa hipótesis en que la nulidad pretendida resulta de la falsedad de la firma autógrafa asentada en el pagaré o voucher que documenta una operación realizada con la utilización de la información contenida en una tarjeta bancaria o en su microchip, que fue analizado por la Primera Sala de la Suprema Corte de Justicia de la Nación, debiera atribuirse al actor, la carga probatoria de demostrar la citada falsedad, en este caso, de la firma electrónica utilizada como mecanismo de validación del citado acto de comercio electrónico.
>
> Lo anterior, porque como ha quedado explicado, la operación tachada de nula no se celebró con la utilización de un número de identificación personal o NIP falso, sino que se verificó con la digitación del número correcto, que habría sido utilizado indebidamente por una persona distinta del titular de la tarjeta, que evidentemente no está facultado para otorgar su voluntad como elemento de existencia del mencionado acto jurídico.

CUARTO. Existencia de la contradicción de tesis. Sentada la exposición de las ejecutorias materia de análisis, debe determinarse a continuación si existe la contradicción de tesis denunciada entre los criterios sustentados por el Segundo Tribunal Colegiado en Materia Civil del Sexto Circuito y el Tercer Tribunal en Materia Civil del Primer Circuito.

Para determinar lo anterior, debe analizarse si los tribunales colegiados contendientes resolvieron alguna cuestión litigiosa en la que tuvieron que ejercer el arbitrio judicial a través de un ejercicio interpretativo con base en argumentaciones lógico jurídicas para justificar su decisión; asimismo, deberá existir una discrepancia entre dichos ejercicios interpretativos, pues 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; y por último, dicha discrepancia deberá dar lugar a la

formulación de una pregunta genuina respecto de si la manera de acometer la cuestión jurídica es preferente con relación a cualquier otra que, como la primera, también sea legalmente posible.

Así lo determinó la Primera Sala de esta Suprema Corte de Justicia de la Nación en la jurisprudencia de rubro siguiente: ***"CONTRADICCIÓN DE TESIS ENTRE TRIBUNALES COLEGIADOS DE CIRCUITO. CONDICIONES PARA SU EXISTENCIA."***[1]

Asimismo, el Pleno de este Alto Tribunal ha determinado que una contradicción de tesis es existente 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.

Lo anterior, con la finalidad de proporcionar certidumbre en las decisiones judiciales y dar mayor eficacia a su función unificadora de la interpretación del orden jurídico nacional. De conformidad con la tesis jurisprudencial 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".***[2]

---

[1] Novena Época, Registro: 165077, Primera Sala, Jurisprudencia, Visible en el Semanario Judicial de la Federación y su Gaceta, Tomo XXXI, Marzo de 2010, Materia(s): Común, Tesis: 1a./J. 22/2010, Página: 122.

[2] Novena Época, Registro: 164120, Pleno, Jurisprudencia, Visible en el Semanario Judicial de la Federación y su Gaceta, Tomo XXXII, Agosto de 2010, Materia(s): Común, Tesis: P./J. 72/2010, Página: 7.

De acuerdo con lo resuelto por el Tribunal Pleno de la Suprema Corte de Justicia de la Nación en sesión de treinta de abril de dos mil nueve, una forma de aproximarse a los problemas que plantean los tribunales colegiados en este tipo de asuntos debe radicar en la necesidad de unificar criterios y no en la de comprobar que se reúna una serie de características determinadas en los casos resueltos por los tribunales colegiados. Por ello, para comprobar que una contradicción de tesis es procedente, se requiere determinar si existe una necesidad de unificación.

En otras palabras, si la finalidad de la contradicción de tesis es la unificación de criterios, y dado que el problema radica en los procesos de interpretación adoptados por los tribunales contendientes, entonces, es posible afirmar que para que una contradicción de tesis sea procedente es necesario que se cumplan las siguientes condiciones[3]:

---

[3] Al respecto, es aplicable la jurisprudencia P./J. 72/2010, del Tribunal Pleno de esta Suprema Corte de rubro y texto siguiente: ”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. 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 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.

1. Los tribunales contendientes debieron haber 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. Entre los ejercicios interpretativos respectivos se debe encontrar algún punto de toque; es decir, que exista al menos un tramo de razonamiento en el que la 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 que sobre ese mismo punto de derecho, los tribunales contendientes adopten criterios jurídicos discrepantes.

3. Que lo anterior pueda dar lugar a la formulación de una pregunta genuina acerca de si la manera de acometer la cuestión jurídica es preferente con relación a cualquier otra que, como la primera, también sea legalmente posible.

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.”.

En atención a dichos criterios, esta Primera Sala considera que **en el caso sí se actualiza la contradicción de tesis**, como se explicará a continuación.

Los **dos primeros requisitos se cumplen** en tanto que en ambos casos los tribunales colegiados contendientes se vieron en la necesidad de analizar 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); siendo que en sus determinaciones llegaron a conclusiones disímiles, en tanto que el **Tercer Tribunal Colegiado en Materia Civil del Primer Circuito** concluyó que cuando se intenta la acción en comento, la institución bancaria demandada sólo debe acreditar -*por cualquier medio de prueba*- que las operaciones que generaron los cargos se realizaron electrónicamente, lo cual revertirá la carga de la prueba a quien niega la transacción, y éste deberá demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad o en su caso, impugnar la certeza de la operación bancaria; mientras que, por el otro lado, el **Segundo Tribunal Colegiado en Materia Civil del Sexto Circuito** arribó a la conclusión contraria, pues consideró que cuando se da el supuesto en estudio, corresponde al banco demandado la carga de la prueba, ya que como operador de los sistemas cibernéticos con que se llevan a cabo las operaciones de comercio electrónico, tiene la obligación de justificar la adopción de todas aquellas medidas de seguridad que den certeza de la operación realizada.

En efecto, el **Tercer Tribunal Colegiado en Materia Civil del Primer Circuito** estimó que, ante una acción de nulidad por desconocimiento de una transacción comercial, la institución bancaria

sólo debe acreditar que se realizaron electrónicamente las operaciones que generaron los cargos por cualquier medio de prueba, siendo carga probatoria de quien niega la transacción, el demostrar que el sistema que utiliza las firmas electrónicas carece de fiabilidad o, en su caso, impugnar la certeza del movimiento bancario.

Para apoyar tal conclusión, refirió qué debe entenderse por firma electrónica y al respecto, transcribió algunas disposiciones del Código de Comercio y de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional; asimismo, hizo alusión a la Guía para la incorporación de la ley modelo mencionada. De ello obtuvo que, el uso de la firma electrónica en las operaciones bancarias constituye una fuente válida de obligaciones para los tarjetahabientes que se vinculan a dicho mecanismo de seguridad para las transacciones comerciales.

En la misma línea, precisó que la ley modelo en comento establece como eje rector de la firma electrónica la fiabilidad en su creación; lo cual otorga certeza a quien la posee que sólo éste puede utilizarla y, por ende, es fuente de obligaciones. Por ello, una vez acreditado el método de creación de la firma electrónica, su ingreso al sistema de datos genera un vínculo jurídico que torna en incuestionable si fue el titular quien utilizó la firma electrónica; siendo que sólo podrá ponerse en duda la fiabilidad del método de creación. Empero, precisó que lo contemplado en la ley modelo debía analizarse en concatenación con lo dispuesto por el artículo 97 del Código de Comercio.

Así, después de referir los datos contenidos en los vouchers, concluyó que la institución bancaria sólo debe acreditar que se

realizaron electrónicamente las operaciones, pues entonces la carga probatoria será de quien niega la transacción, el cual deberá demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad o en su caso, impugnar la certeza de la operación bancaria. Máxime que, las normas sobre firmas electrónicas califican de válidos los actos jurídicos donde se ingrese este tipo de firmas sin cuestionar la fiabilidad del método de uso, sino sólo el de creación. Por tanto, la parte que cuestiona la certeza y validez de la transacción tiene la carga de acreditar que no se utilizó en dicha operación la tarjeta ni el PIN personal con los que se realizó el movimiento bancario.

Para reforzar tal conclusión, el tribunal colegiado distinguió entre la fiabilidad de la firma electrónica y la certeza de la operación bancaria como fuente de obligaciones.

En cuanto a la fiabilidad de la firma electrónica resaltó que el artículo 6 de la ley modelo, acogido por el artículo 97 del Código de Comercio, señalan los requisitos que debe contener la creación de una firma electrónica para considerarla fiable. Respecto la certeza de la operación, señaló que sus elementos materiales, es decir, la seguridad en quien realizó la operación es el titular de la firma electrónica; no encuentran sustento en su ámbito personal, sino en la utilización del *password* o PIN, ya que los medios electrónicos que se utilizan como la terminal punto de venta y el sistema operativo que traduce la información, derivan de fuentes internacionalmente aceptadas y, consecuentemente, su cuestionamiento compete a quien lo pone en tela de juicio bajo el principio ontológico de la carga de la prueba, según el cual lo ordinario se presume y lo extraordinario se prueba, siendo lo ordinario que las terminales y el sistema operativo no sean vulnerables, por ende, corresponde la carga de la prueba a quien alega lo contrario.

Por su parte, el **Segundo Tribunal Colegiado en Materia Civil del Sexto Circuito**, concluyó que cuando se haga valer la acción en estudio, la carga probatoria le corresponde al banco demandado, pues como operador de los sistemas cibernéticos con que se llevan a cabo las operaciones de comercio electrónico, tiene la obligación de justificar la adopción de todas aquellas medidas de seguridad que den certeza de la operación realizada.

Durante el desarrollo de su estudio, el órgano colegiado refirió que en el caso concreto la problemática derivó de una clonación de tarjeta bancaria, en relación con la cual resultaba complejo establecer a quién le correspondía la carga probatoria, pues para ello, primero debía identificarse qué era lo que sería posible de ser justificado, ya que de lo contrario se asignarían obligaciones de difícil o incluso de imposible cumplimiento.

A partir de la identificación de los distintos extremos que podrían considerarse al momento de hacer la asignación o distribución de las cargas probatorias, concluyó que no pueden tomarse en cuenta sólo las reglas generales contenidas en el Código de Comercio, sino también las relativas a la posibilidad o menor dificultad para justificar los citados elementos, ponderando la especial condición de cada una de las partes, así como la forma en que se relacionan al contratar y realizar operaciones de banca electrónica, y en función de ello la mayor o menor posibilidad de justificar el hecho materia de discusión.

Con base en ello, determinó que a nada práctico conduciría atribuir a la persona que se dice víctima, la obligación de demostrar tal evento, es decir, que los elementos que permitirían identificarlo electrónicamente, tanto con una cuenta bancaria, a partir de la

información contenida en la cinta magnética o microchip incorporado a una tarjeta de débito o de crédito, como con el número de identificación asociado a ella, que fueron idénticamente reproducidos, pues la conclusión sería la misma, esto es, que la operación electrónica objetada se llevó a cabo mediante la utilización de la información que el banco otorga a sus clientes, al momento en que les entrega sus respectivas tarjetas y se genera la firma electrónica correspondiente; lo cual anularía por completo la posibilidad de éxito de la acción.

Por tanto, consideró que el problema se circunscribe en que esa información, la cual es confidencial, no se vuelva vulnerable. Y si lo es, que se adopten todas aquellas medidas que permitan evitar su indebida o ilícita utilización.

De allí que, si en este tipo de casos, los aparatos o mecanismos -terminal- son manipulados por seres humanos, entonces el receptor del citado medio electrónico de pago, -como sana práctica mercantil, y por seguridad tanto de la operación como de quienes en ella intervienen- debe constatar la identidad de quien pretende hacer uso de la tarjeta, por lo que razonablemente se le puede exigir como condición para aceptar el citado mecanismo de pago, solicite algún documento oficial que sirva como identificación de quien lo utiliza o pretende utilizarlo, a efecto de corroborar que se trate del titular de la cuenta asociada a la respectiva tarjeta bancaria, pudiendo consignarse el nombre o forma de identificar a la persona que utiliza la tarjeta bancaria que sirve como medio electrónico de pago, a fin de corroborar de la legitimación del usuario que interviene en el acto de comercio.

Con base en lo anterior, concluyó que al resultar razonable la obligación indicada a quien celebra una operación de comercio electrónico, entonces se puede establecer la distribución de cargas probatorias, pues debía de constatarse la identidad de la persona que al amparo de una tarjeta bancaria pretende celebrar un acto mercantil, como forma o mecanismo que conduzca a la certeza del acto cuestionado. Por tanto, la carga de la prueba le corresponde al banco demandado, pues como operador de los sistemas cibernéticos con que se llevan a cabo las operaciones de comercio electrónico, tiene la obligación de justificar la adopción de todas aquellas medidas de seguridad que den certeza de la operación realizada, es decir, de que fue llevada a cabo por el titular de la cuenta bancaria contra la que se efectúa el cargo cuestionado.

Es decir, el banco demandado puede diseñar un sistema que permita conocer la identidad de la persona portadora de una tarjeta bancaria, que es utilizada en una terminal, tan solo con permitir que su nombre aparezca visible en la impresión del comprobante de esa operación, conocido como voucher o pagaré, y esto último, es lo que haría posible que la persona que opera la mencionada terminal, esté en condiciones de solicitar a quién le entrega la tarjeta, su identificación para constatar que se trate del titular de la cuenta o de persona autorizada en ella por este. De lo contario, estaría facultado para rechazar la operación pretendida (o celebrarla bajo su riesgo), pero no a cuenta de quién no es titular del derecho bancario para hacer uso lícito de una tarjeta y de la firma asociada a ella.

Ahora bien, una vez precisado lo anterior, esta Primera Sala considera que también se actualiza el **tercer requisito,** en torno *“a la formulación de una pregunta genuina acerca de si la manera de acometer la cuestión jurídica es preferente con relación a cualquier*

otra que, como la primera, también sea legalmente posible"; pues en el caso se considera oportuno, en aras de la seguridad jurídica, clarificar 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).

No es óbice para la existencia de la presente contradicción, el hecho de que el **Tercer Tribunal Colegiado en Materia Civil del Primer Circuito** arribara a lo conclusión de que al cliente le corresponde la carga de la prueba, con base en que el NIP al ser una firma electrónica -una vez acreditado su método de creación, su ingreso al sistema de datos- genera un vínculo jurídico que torna en incuestionable si fue el titular quien utilizó la firma electrónica; pues consideró que sólo podría ponerse en duda la fiabilidad del método de creación, resaltando los requisitos que debe contener la creación de una firma electrónica para considerarla fiable de conformidad con el artículo 97 del Código de Comercio. En cambio, el **Segundo Tribunal Colegiado en Materia Civil del Sexto Circuito** aclaró que no era materia de estudio los elementos de lo que se denomina *"Firma Electrónica Avanzada"* o *"Firma Electrónica Fiable"*, regulada en el artículo 97 del Código de Comercio, cuyos elementos constitutivos, de creación, validación y constatación en cuanto a su existencia y corrección, son distintos de los que se utilizan al momento en que se genera un número de identificación personal o NIP que se asocia a una tarjeta bancaria.

Lo anterior es así, puesto que si bien podría considerarse que los tribunales colegiados partieron de premisas diversas -consistente en la naturaleza del NIP y si éste constituye o no una firma electrónica

avanzada, pues uno decidió otorgarle fiabilidad a su creación, mientras que el otro órgano colegiado no tomó en consideración esa circunstancia-, y por ello llegaron a conclusiones diversas en cuanto a quién le correspondía la carga de la prueba; lo cierto es que ambos tribunales colegiados analizaron la misma situación fáctica, pues conocieron de asuntos donde se reclamó la nulidad del voucher o pagaré emitido al amparo de una tarjeta bancaria, siendo que el consentimiento se plasmó mediante el uso de un NIP, sosteniendo ambos demandantes que los cargos derivados de las operaciones comerciales fueron efectuados por personas diversas a los cuentahabientes.

De allí que, lejos de declarar la inexistencia de la presente contradicción, se considera que en aras de salvaguardar el principio de seguridad jurídica, en primer lugar se deberá dilucidar si el NIP que se asocia a una tarjeta bancaria, con el cual puede realizar operaciones comerciales, constituye una firma electrónica; y una vez sentado lo anterior, explicar 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).

En esos términos esta Primera Sala considera que sí existe la contradicción de tesis, y por lo tanto, procederá al estudio de fondo.

QUINTO.- Criterio que debe prevalecer. Debe prevalecer con carácter de jurisprudencia el criterio sustentado por esta Primera Sala de la Suprema Corte de Justicia de la Nación, consistente en que cuando se demanda la nulidad de los vouchers emitidos con motivo del uso de una tarjeta bancaria autorizados mediante la digitación de

un número de identificación personal (NIP), y el usuario niega haber realizado los pagos que originaron los cargos cuya cancelación demandó, es la institución bancaria quien está obligada a ofrecer las pruebas pertinentes con las que se acredite que fue el propio usuario quien realizó dicha transacción, de conformidad con las siguientes consideraciones.

En primer lugar, debe indicarse que el presente estudio se dirige únicamente a supuestos en los cuales una persona realiza una compra en un establecimiento comercial, y efectúa el pago mediante una tarjeta bancaria, siendo que para confirmar los cargos digita un número de identificación personal (NIP).

Ahora bien, a fin de poder resolver la materia de análisis de la contradicción de criterios que ahora nos ocupa, como punto de partida es necesario explicar ciertos temas afines con la problemática que se presenta en relación con las operaciones bancarias derivadas de intercambios de información electrónica en el sistema financiero mexicano, como son: **a)** comercio electrónico en México**, b)** firma electrónica y naturaleza jurídica del número de identificación personal, **c)** seguridad en actos de comercio electrónico, **d)** cargas probatorias, y **e)** conclusión.

a) Comercio electrónico en México.

El desarrollo de diversas tecnologías de información, así como el crecimiento exponencial de las telecomunicaciones y el fortalecimiento de globalización e interdependencia económicas, dieron origen a formas novedosas para realizar la actividad comercial, donde tanto oferentes como demandantes empezaron a efectuar sus transacciones a través de medio electrónicos.

Así, el uso constante de la tecnología para realizar actos jurídicos ha dado origen al comercio electrónico, el cual consiste en el conjunto de actos de intermediación de bienes y servicios a través de mensajes de datos, transmitidos por medios electrónicos, ópticos o similares (internet, correo electrónico, intercambio electrónico de datos, facsímil o télex)[4].

Tal uso constante de la tecnología para realizar actos jurídicos, así como la preferencia y algunas veces la necesidad de los usuarios, ha propiciado una evolución semántico-jurídica del concepto de documento ampliado para cubrir al documento digital o mensaje de datos, así como la realización de operaciones y ofertas por medio de mensajes de datos.[5] Sin embargo, aunque este tipo de operaciones son comunes en nuestro día a día, no deja de preocupar que el documento digital no sea tangible, lo que genera inseguridad para las personas que interaccionan en las actividades realizadas con tales medios.

Generalmente, desde la invasión de la era digital, los avances tecnológicos llegan frecuentemente, con antelación a la legislación que regula su uso; es por ello que, para vislumbrar la importancia que ha tenido el comercio electrónico, resulta importante hacer alusión a que en nuestro país, antes del año dos mil, prácticamente no existían normas que reconocieran de manera expresa la validez de las operaciones realizadas por medios electrónicos, ópticos o similares.

Así es, debido a que las operaciones por medios electrónicos se empezaron a practicar en forma significativa a mediados de la década

---

[4] León Tovar, González García y Vázquez del Mercado Blanco, *La firma electrónica avanzada: estudio teórico, práctico y técnico,* Oxford, México 2006, p.25.
[5] *Ibídem.*

de los noventa, en nuestro país se reconoció la equivalencia funcional de la información contenida en papel con la información contenida en ciertos archivos telemáticos y electrónicos o de tecnologías similares, facilitados con la comunicación y envío de información a través primero del intercambio de datos electrónico, luego del fax, internet, el correo electrónico y otros medios electrónicos[6].

Ante ese panorama, fue el Código de Comercio el ordenamiento que tuvo reformas más significativas en ese rubro. Tales reformas se gestaron en el año de mil novecientos noventa y nueve, mediante tres iniciativas, con la injerencia de organismos nacionales tanto públicos como privados.

Desde un principio, el poder legislativo buscó adoptar la Ley Modelo sobre Comercio Electrónico realizada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, a nuestro derecho interno, tal como se observa en la exposición de motivos de la Cámara de Diputados de fecha veintinueve de abril de mil novecientos noventa y nueve:

> *"Desde el origen de las civilizaciones el comercio ha sido una actividad importante, ya que mediante él, los seres humanos han podido intercambiar bienes y servicios entre sí. Esta actividad requiere para su eficaz desarrollo de la confianza que da la certeza. En la actualidad esto se alcanza con los registros escritos, es decir, con registros tangibles. Bajo este esquema de consignación de documentos en papel, los conceptos de "original" y "firma" cobran gran importancia, siendo los únicos vehículos para la autenticación de las relaciones comerciales.*
>
> *Sin embargo, el rápido desarrollo de los sistemas informáticos y de comunicación han llevado a buscar maneras más rápidas para llevar a cabo la actividad comercial. Los medios electrónicos modernos (principalmente el internet y el correo electrónico) han logrado acortar las distancias y los plazos de orden y entrega entre los participantes de la actividad comercial, logrando mayor*

[6] *Ibídem*, p. 38.

eficiencia en los procesos del ramo, beneficiando a la economía en general.

Ante este vertiginoso cambio, la legislación comercial y la lex mercatoria han sido rebasadas, creándose así barreras u obstáculos, en razón de lagunas legales para el comercio, como es el uso de las consignaciones en papel. Para poder realizar este tipo de transacciones electrónicas es necesario modernizar la ley comercial a fin de que al momento de llevar esta actividad, no solamente se contemplen documentos materiales, sino que se contemplen como medios jurídicamente válidos los documentos enviados por la vía electrónica.

Para la elaboración de la presente iniciativa se tomó la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) en Comercio Electrónico como base jurídica y se analizó el contexto, la legislación y la práctica comercial mexicana, para lograr que se adaptara de manera precisa a la realidad nacional. Lo anterior trae como consecuencia que el derecho internacional en materia de comercio electrónico sea compatible con el régimen mexicano de comercio electrónico, permitiendo así mayor seguridad y certeza en las transacciones electrónicas tanto nacionales como internacionales. La Ley Modelo del Comercio Electrónico, que es una serie de normas jurídicas de carácter internacional creadas para ser estudiadas, adaptadas y aplicadas a nivel local por los Congresos de los diferentes países del orbe, está diseñada con el afán de lograr un derecho "global", en el cual las reglas jurídicas sean similares entre las diferentes naciones. En particular, la Ley Modelo de Comercio Electrónico se ha aplicado exitosamente en la República de Corea, Singapur y dentro de los Estados Unidos de América en el estado de Illinois.

En el marco de esta modernización a las leyes comerciales buscado por la presente iniciativa, la cual integra el comercio electrónico, se logran dos metas:

** Eliminar los obstáculos existentes para el comercio electrónico, ajustando la práctica comercial con la ley en dicha materia, e*

** Incluir los avances y características específicas relacionadas con el comercio electrónico, como es la posibilidad de acceder a los productos en fotos vía internet sin necesidad de tener el producto físicamente presente para evaluarlo*

Dicha actualización legislativa se da en esta iniciativa bajo un marco de "neutralidad del medio", es decir, eliminando las barreras al comercio electrónico, sin modificar los requisitos existentes en cuanto a los documentos en papel.

La importancia de estas reformas emana de una realidad, del hecho de que los medios de comunicación modernos -tales como el correo electrónico y el intercambio electrónico de datos- han difundido su uso con gran rapidez en las operaciones comerciales tanto nacionales como internacionales, lo que hace presumir que este tipo de comunicación será preponderante en el futuro próximo. Dado que la actividad comercial es vital para la vida de México, es necesaria su constante actualización, por lo que la presente iniciativa se enfoca a crear un marco jurídico que permita una sana integración y desarrollo del comercio por la vía electrónica, es decir, de una realidad a la normatividad.

Considerando lo obsoleto de la actual legislación comercial, la presente iniciativa constituye un instrumento para reglar ciertos convenios comerciales fijando un mínimo de requisitos o características que deben tener los documentos para ser considerados con pleno valor probatorio. La iniciativa logra lo anterior mediante la utilización del concepto del "equivalente funcional" entre los documentos consignados en papel y aquéllos consignados por vía electrónica. Este concepto hace posible establecer una serie de características que dan a la documentación, vía medios electrónicos, un grado de seguridad similar al de la documentación consignada en papel.

Al mismo tiempo, la presente iniciativa busca permitir o facilitar el comercio electrónico dando igualdad de trato a los contratos que tengan soporte informático con relación a aquéllos que lo basen en documentación consignada en papel. Esto indudablemente busca una mejoría para la actividad comercial en general y la economía mexicana en su conjunto, agiliza las transacciones comerciales y logra una mejor vinculación con los mercados extranjeros, pues tanto los productores como los consumidores extranjeros ven al comercio electrónico como un fenómeno cotidiano.

*El establecer un régimen de comercio electrónico conlleva una serie de características nuevas que la legislación debe contemplar y regular. Tal es el caso de la firma electrónica, la cual representa el consentimiento de una de las partes para la realización de una cierta acción**. Sin un régimen de firmas electrónicas y métodos confiables para la autenticación de las mismas se hace más difícil la actividad del comercio electrónico.** Es por ello que, a manera de complemento, se introduce el Título Primero dentro de esta iniciativa, en el cual se presentan los lineamientos generales para la utilización y verificación de las firmas electrónicas.*

Este régimen de firmas electrónicas también está adaptado a partir de un documento de la CNUDMI (el Proyecto de Régimen Uniforme para las Firmas Electrónicas) y continúa con la tónica

> *presentada en la parte de la iniciativa referente al comercio electrónico al mantener la "neutralidad del medio", es decir, al no desalentar el uso de otras técnicas de autenticación de la voluntad, tal como la firma de puño y letra. Al mismo tiempo, presenta la figura de las entidades certificadoras, que tienen la función de dar seguridad al régimen al corroborar la autenticidad de una firma electrónica en caso de que alguna de las partes no confíe en la originalidad de la misma. Estas entidades podrán pertenecer a la iniciativa privada, fomentando la creación de organismos con alta especialización tecnológica así como nuevas fuentes de empleo.”.*

De la iniciativa transcrita con anterioridad se desprende que, a fin de mejorar el fortalecimiento de la actividad comercial y atendiendo al crecimiento exponencial en las operaciones comerciales tanto nacionales como internacionales, era importante la implementación de diversos mecanismos que abordaran la regulación en el uso de los medios de comunicación modernos -tales como el correo electrónico y el intercambio electrónico de datos-, precisamente por la presunción de que este tipo de herramientas serían preponderantes a futuro para agilizar todo tipo de transacciones.

De igual forma, se advierten dos metas específicas que se pretendieron alcanzar con la iniciativa aludida:

1. Eliminar los obstáculos existentes para el comercio electrónico, ajustando la práctica comercial con la ley en dicha materia; e,

2. Incluir los avances y características específicas relacionadas con el comercio electrónico, como es la posibilidad de acceder a los productos en fotos vía internet sin necesidad de tener el producto físicamente presente para evaluarlo.

Como ha quedado precisado, para la elaboración de la iniciativa se tomó como base jurídica la Ley Modelo de la Comisión de las

Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico; de la cual se extrajo el concepto de "*equivalente funcional"*, el cual hace posible establecer una serie de características que dan a la documentación, vía medios electrónicos, un grado de seguridad similar al de la documentación consignada en papel, dicho concepto también permite considerar los documentos digitales con pleno valor probatorio.

Debe destacarse que, a fin de hacer frente a la evidente complejidad que conllevaba adoptar las reglas del comercio electrónico, la iniciativa de reforma indicada, se complementó con las diversas reformas presentadas ante la Cámara de Diputados el quince de diciembre de mil novecientos noventa y nueve y veintidós de marzo de dos mil, respectivamente, en las que se proponían adiciones al Código de Comercio para incorporar dentro del Libro Segundo relativo al comercio terrestre un Título II, denominado *"Del Comercio Electrónico"*.

El veintinueve de abril de dos mil, fueron aprobadas las reformas al Código de Comercio, las cuales entraron en vigor a los nueve días siguientes de su publicación en el Diario Oficial de la Federación el veintinueve de mayo de dos mil; en las que ya se reconocía la equivalencia funcional entre la información contenida en papel y la información contenida en un mensaje de datos; empero, no había seguridad ni certeza jurídica de poder acudir a los tribunales exitosamente para exigir el cumplimiento de las obligaciones derivadas de un contrato celebrado vía electrónica.

En virtud de lo anterior, se añadió al Código de Comercio un título especial, reestableciendo algunos de los artículos anteriormente derogados del Libro Segundo, tomando en cuenta la necesidad de

regular de manera específica la contratación a distancia, o aquella en que las partes no están físicamente presentes; así como para reconocer dichas operaciones y dar valor probatorio al uso de medios electrónicos en los procesos administrativos y judiciales, sin que pueda quedar al arbitrio del juez considerar su validez probatoria en caso de controversia.

Pese al exhaustivo trabajo efectuado en el proceso legislativo materializado en las reformas en comento, sólo se adoptó parcialmente la Ley Modelo sobre Comercio Electrónico, omitiéndose aspectos importantes previstos en esa ley y lo relativo a las firmas electrónicas. Dicha omisión, trajo como consecuencia la necesidad de adaptar nuevamente la legislación en relación con la materia de firma electrónica, lo que aconteció mediante reforma de veintinueve de agosto de dos mil tres, donde se adicionó al capítulo referente al Comercio Electrónico, la Ley Modelo sobre Comercio Electrónico y la Ley Modelo sobre Firmas Electrónicas, ambas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional y, con ello, establecer la necesidad de contar con una firma electrónica y prever la existencia de instituciones certificadoras de dichos instrumentos.

Hasta aquí un breve esbozo de cómo, ante el inminente uso de los medios electrónicos para realizar actos jurídicos, se comenzó a regular el comercio electrónico en nuestra legislación.

b) Firma electrónica.

Si bien es cierto que el uso del dinero en efectivo continúa siendo una forma de pago clave en nuestro país y la firma autógrafa es el medio por excelencia para crear vínculos entre las partes que intervienen en la celebración de actos jurídicos; también lo es que

existe una reducción significativa en su uso, en atención a que actualmente un gran número de transacciones comerciales para el pago de algún servicio o para la adquisición de algún bien, se realizan mediante el comercio electrónico. Como herramienta para facilitar la realización de dichas operaciones -regularmente- los consumidores utilizan tarjetas bancarias.

En efecto, a fin de agilizar el tráfico comercial, entre los proveedores de bienes y servicios y sus clientes, las instituciones financieras han adoptado un sistema de tarjetas, esto es, el empleo de una pieza de plástico que contiene información física y electrónica que identifica a la entidad emisora, al afiliado autorizado para emplearla, los recursos con que cuenta este último, ya sean propios y que tenga disponibles en su cuenta (débito) o los de la institución financiera de los cuales se hace cargo y luego cobra al cliente a cambio del cobro de un interés (crédito); el periodo temporal en el que ese instrumento mantendrá su vigencia y la firma del portador legítimo.

Las actividades mercantiles que se realizan con base en el uso de tarjetas como instrumento bancario de pago son complejas, ya que se realizan diferentes relaciones entre los sujetos que intervienen, esto es, el tarjetahabiente adquiere los bienes y servicios que ofrece el vendedor y es la entidad financiera la que se hace cargo del pago a este último (a través de las operaciones ya sea de crédito o débito que tenga con su cliente) previo la promesa formulada por el referido tarjetahabiente a la entidad emisora de la tarjeta a través de un documento denominado voucher, el cual cumple las funciones de un pagaré, de abonar el precio de las compras efectuadas según las modalidades pactadas entre ellos.

En estos casos, la persona autorizada por el vendedor para realizar la transacción usualmente tiene a su alcance una terminal punto de venta mediante la cual realiza el cobro del bien a cargo de la tarjeta bancaria, mientras que el consentimiento del tarjetahabiente comprador se expresa, ya sea por su firma autógrafa o, en su defecto, por la introducción de un número de identificación personal (NIP). En caso de ser aprobada la venta por parte del banco otorgante de la tarjeta, emitirá un comprobante o voucher donde conste fehacientemente la autorización o declinación de la compraventa.

Como ha quedado asentado, dado que no sólo en relación con las cargas probatorias cuando se ejerce la acción de nulidad de vouchers emitidos por transacciones comerciales realizados con tarjetas bancarias autorizadas mediante número de identificación personal (NIP), existe discrepancia de criterios entre los tribunales colegiados contendientes; a fin de privilegiar la seguridad jurídica, esta Primera Sala también debe pronunciarse respecto a si tal número de identificación constituye o no una firma electrónica, a partir de los razonamientos siguientes:

El artículo 89 del Código de Comercio, define a la firma electrónica de la siguiente manera:

> *“Art. 89. (…) Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones: (…)*
> *Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio…”.*

Como puede advertirse, para el Código de Comercio la firma electrónica consiste en los datos consignados, adjuntados o asociados en un mensaje de datos, los cuales sirven tanto para identificar al firmante, como para indicar que este aprueba la información contendida en el mensaje de datos.

Dada la definición referida, debemos dilucidar qué es un mensaje de datos. En ese sentido, el propio numeral 89 nos otorga una definición:

> *"(…) Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología...".*

Por su parte, la Ley Modelo sobre Comercio Electrónico -misma que fue referencia para nuestro legislador-, define al mensaje de datos de la siguiente manera:

> *"[…] a) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI)*[7]*, el correo electrónico, el telegrama, el télex o el telefax;…".*

De lo cual se sigue que un mensaje de datos engloba a todo tipo de información generada, enviada, recibida, archivada o comunicada mediante algún medio electrónico, óptico o similar, es decir, por cualquier medio diverso al papel. A su vez, como ya se indicó, el comercio electrónico es el conjunto de actos de intermediación de bienes y servicios a través de mensajes de datos, transmitidos por

[7] En la misma ley modelo que se comenta se define al intercambio electrónico de datos de la siguiente manera: *b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto*;

medios electrónicos, ópticos o similares (internet, correo electrónico, intercambio electrónico de datos, facsímil o télex).

Con base en tales premisas, podemos afirmar que indefectiblemente un acto de comercio electrónico conlleva la utilización de una firma electrónica, pues solo así puede existir un consentimiento del acto por parte del firmante.

Ahora, en lo que aquí interesa, vale la pena señalar que un gran número de actos de comercio se realizan mediante vías de transmisión basadas en técnicas electrónicas, siendo que dentro de ellas la más ocupada es la comunicación por medio del intercambio de datos electrónico[8], por tanto, es importante explicar cómo se desenvuelve.

El artículo 2 de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico, nos presenta la siguiente definición de intercambio de datos:

> *"… b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;…".*

De lo anterior, se colige que el intercambio de datos es el envío y recepción de documentos a través de medios telemáticos con el fin de posibilitar su tratamiento automático. Este sistema pretende que el

[8] Resolución aprobada por la Asamblea General de la CNUDMI: *"(…) Observando que un número creciente de transacciones comerciales internacionales se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación, habitualmente conocidos como "comercio electrónico", en los que se usan métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel,...".*

emisor y el receptor de un determinado documento puedan estar directamente frente a las computadoras respectivas, ganando así tiempo y evitando errores, sin que ello implique que los actos se atribuyan a la computadora, sino a la persona a cuyo nombre se ha programado la misma.[9]

El intercambio de datos está considerado un servicio de valor agregado que consiste en proporcionar a los usuarios el almacenamiento y envío automatizado de información estructurada bajo un formato definido.[10]

Así, mediante el intercambio electrónico puede transmitirse información a la par del correo electrónico, internet y en general de las redes de telecomunicaciones; así como mensaje de datos el cual puede contener la identificación de una firma electrónica.

Cabe mencionar que, el intercambio de datos electrónico, comprende tres tipos de transmisión:

1. La transmisión de datos de una terminal informática a otra utilizando un formato normalizado.
2. La transmisión de mensajes electrónicos mediante el uso de normas patentadas o normas de libre acceso, y
3. La transmisión por vía electrónica de textos de formato libre utilizando medios como internet, el correo electrónico, el télex, la telecopia[11] o el fax.

---

[9] León Tovar. *Op. cit.* p. 60.
[10] *Ibídem*.
[11] *"La transmisión a distancia de textos de un terminal a otro se ha hecho posible con la conexión de los sistemas informáticos a las redes de telecomunicaciones (sea al teléfono, sea a una red especializada de transmisión). Por medio de las redes que conectan los ordenadores se pueden establecer contactos permanentes y transmitir mensajes electrónicos, que aparecen en la pantalla de la persona con quien uno se comunica."*

En ese sentido, podemos concluir que la firma electrónica se constituye por los datos aparejados a un mensaje de datos, el cual debe entenderse como la información generada, enviada, recibida, archivada o comunicada mediante algún medio electrónico, y entre tales medios se encuentra el intercambio de información estructurada bajo alguna norma técnica o formato convenido; la cual sirve para identificar al firmante y vincular su consentimiento con el acto comercial que se realiza.

Tomando en consideración el desarrollo el sistema financiero y la protección de los intereses de los usuarios, el Banco de México incentivó a las instituciones financieras emisoras de tarjetas bancarias para que adoptaran las medidas adicionales a fin de reducir riesgos derivados del uso de tales instrumentos en transacciones comerciales[12]. A raíz de lo anterior, la gran mayoría de las instituciones bancarias han optado por sustituir la firma autógrafa para sus clientes, con el uso obligatorio del NIP, como herramienta de autenticación en las operaciones comerciales de los tarjetahabientes.

Así, cuando una persona acude a una institución financiera con la finalidad de obtener una tarjeta bancaria -sea de crédito o débito- (sin entrar en detalle en relación con el tipo de contrato que la originó) durante el trámite, la institución financiera solicita al cliente digitar un número que servirá de identificación personal para realizar diversos actos para el adecuado manejo de su cuenta.

November, András. (1990) Nuevas Tecnologías y Transformaciones Socioeconómicas. Manual de Nuevas Tecnologías. 1ª Ed. Madrid. Hermanos García Noblejas, p. 47.

[12] CIRCULAR 34/2010, dirigida a las Instituciones de Banca Múltiple, Sociedades Financieras de Objeto Limitado y Sociedades Financieras de Objeto Múltiple Reguladas relativa a las Reglas de Tarjetas de Crédito.

El NIP es un número confidencial compuesto regularmente por cuatro dígitos, elegidos por el cliente, y se trata de una clave con la cual lo identifica ante el sistema del banco, utilizado para:

1. Realizar operaciones en los cajeros automáticos.
2. Utilizar la banca electrónica.
3. Hacer pagos de productos o servicios.

Como se indicó, el número de identificación personal ha venido a sustituir la firma autógrafa, ya que por medio del tecleo[13] de los dígitos que lo conforman se pueden adquirir productos o servicios en establecimientos comerciales, vinculando al firmante con el acto efectuado. En otras palabras, cuando en un comercio se pretende adquirir un producto utilizando como medio de pago una tarjeta bancaria, el comprador debe aprobar esa transacción mediante la manifestación de su voluntad, exteriorizada en la digitación de su NIP, el cual sustituye a la firma autógrafa que se plasmaba en el voucher[14] o comprobante que se emite con motivo de la operación.

La definición del número de identificación personal, la encontramos en las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito[15], cuyo artículo primero establece:

> *"CXV. Número de Identificación Personal (NIP): a la Contraseña que autentica a un Usuario en el servicio de Banca Electrónica mediante una cadena de caracteres numéricos…".*

---

[13] Nos referimos al tecleo en una terminal punto de venta, porque ese fue el supuesto concreto que tuvieron a la vista los tribunales colegiados contendientes.

[14] El comprobante de pago o voucher es definido por la Real Academia Española de la siguiente manera: *"Vale que da derecho a quien lo posee a adquirir determinados artículos o a disfrutar de un servicio".*

[15] Las Disposiciones de carácter general aplicables a las Instituciones de Crédito fueron creadas 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, mismas que han tenido diversas modificaciones, siendo la última de ellas la publicada el veintiséis de junio de dos mil dieciocho.

Al respecto debemos referir que las propias Disposiciones definen a la Banca Electrónica de la siguiente manera:

> *"XIV. Banca Electrónica: al conjunto de servicios y operaciones bancarias que las Instituciones realizan con sus Usuarios a través de Medios Electrónicos.".*

No está por demás destacar, que por Banca Electrónica no sólo debe entenderse al portal de las Instituciones en el cual comúnmente el usuario maneja electrónicamente sus cuentas o paga servicios, sino al conjunto de servicios y operaciones bancarias que las instituciones realizan con sus Usuarios a través de medios electrónicos, dentro de las cuales se encuentra el supuesto que aquí se estudia consistente en la adquisición de bienes y servicios.

Con base en lo expuesto, se puede concluir que la naturaleza jurídica del número de identificación personal es la de una firma electrónica simple de conformidad con el artículo 89 del Código de Comercio, pues como se ha explicado, la firma electrónica son los datos consignados, adjuntados o asociados en un mensaje de datos, los cuales sirven tanto para identificar al firmante, como para indicar que éste aprueba la información contendida en el mensaje de datos.

En ese sentido, si el número de identificación personal sirve para vincular al firmante con la operación realizada, pues éste sustituye a la firma autógrafa que antes se requería como símbolo inequívoco de la exteriorización de la voluntad, puede concluirse que adquiere la naturaleza jurídica de una firma electrónica.

c) Funcionamiento de las tarjetas bancarias que cuentan con mecanismos de seguridad Chip y NIP (número de identificación personal).

Una vez definida la naturaleza de la firma electrónica, es menester hacer énfasis en la funcionalidad y vulnerabilidades de las tarjetas bancarias que, como mecanismo de seguridad, cuentan con chip y un número de identificación personal, mejor conocido como NIP.

Los mecanismos denominados “Chip” y “NIP” fueron diseñados para mitigar las vulnerabilidades en las tarjetas de banda magnética, aunque con costos más altos, lo que requirió la actualización de mucha infraestructura con la que contaban previamente las instituciones bancarias. Actualmente, las tarjetas bancarias incluyen una banda magnética y las mismas funciones de seguridad visibles que antes, pero incorporan un chip de computadora adicional debajo de la superficie de las tarjetas.

Un terminal puede interactuar con el chip a través de contactos eléctricos en la cara de la tarjeta. El chip es una computadora con una potencia de procesamiento comparable a la de las computadoras de escritorio de la década de los ochentas, pero con una funcionalidad de seguridad adicional. Este instrumento tiene un programa cargado que es diseñado para seguir las convenciones de comunicación (un protocolo) especificado por la documentación EMV[16], y así poder comunicarse con terminales que cumplan con dicho estándar EMV.

El chip realiza tres operaciones principales: ***I)*** la autenticación de la tarjeta, mediante el cual se establece que la tarjeta es auténtica, ***II)*** verificación del titular de la tarjeta, por la que se establece que la persona que presenta la tarjeta es el titular autorizado de la cuenta, y ***III)*** autorización de transacción, estableciendo que existen suficientes

[16] Esta documentación se denomina EMV, pues hace referencia a los diseñadores de la medida de seguridad “Europay, Mastercard y Visa”.

fondos para completar la transacción y la tarjeta no ha sido cancelada.[17]

I) **Autenticación de la tarjeta.** El objetivo de la autenticación con tarjeta es permitir al operador de una terminal de punto de venta (el comerciante) para establecer si la tarjeta presentada es legítima, sin contactar con el editor. Esto es importante porque existe una pequeña proporción de las transacciones de terminales punto de venta que se realizan cuando la terminal está fuera de línea, por lo que no existiría una comunicación directa con el emisor hasta después de que la mercancía ya ha sido adquirida por el cliente.

Durante la autenticación de tarjeta en terminal punto de venta, la propia tarjeta envía un certificado criptográfico a la terminal, incorporando el número de cuenta de la tarjeta y una firma digital. Así, la terminal puede comprobar si el certificado fue emitido por un banco reconocido por un sistema de pago (por ejemplo, Visa o Mastercard) soportada por el terminal, y validar la firma digital.[18]

II) **Verificación del titular de la tarjeta.** El proceso comienza con un mecanismo de negociación, realizado entre la tarjeta y la terminal punto de venta, para establecer qué método de autenticación pueden (o deben) usar para la verificación del tarjetahabiente. Una vez que el comerciante está convencido de que la tarjeta es auténtica, tanto el

[17] Murdoch Steven J. (2009). *"Reliability of Chip and PIN evidence in banking disputes"*. Digital Evidence and Electronic Signature Law Review, Vol. 6". Pario Communications Limited. Recuperado de: https://murdoch.is/papers/deaeslr09reliability.pd.

[18] Murdoch Steven J, Drimer Saar, Anderson Ross y Bond Mike. "Chip and PIN is broken". University of Cambridge, Computer Laboratory, UK. Recuperado de: https://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf

sistema de la propia tarjeta como el comerciante deben estar seguros de que la persona que presenta el plástico es el propietario de la cuenta legítima. Aquí entra en juego el papel de la verificación del titular de la tarjeta, que normalmente se logra mediante el uso de un NIP (número de identificación personal).

El cliente primero introduce su NIP en un dispositivo de entrada NIP, adjunto a la terminal punto de venta. El número de identificación es enviado a la tarjeta y la tarjeta compara el NIP con el que almacena la institución financiera, y devuelve el resultado del comparativo a la terminal. Si el número introducido es incorrecto, la tarjeta permitirá volver a intentar la entrada del NIP, pero sólo hasta un número máximo de intentos, que regularmente son tres.

III) **Autorización de transacción.** Una vez autenticada la tarjeta y verificado su titular de forma exitosa, el paso final es la autorización de transacción, donde el emisor, la tarjeta y el comerciante pretenden verificar la operación, además de que la tarjeta no ha sido cancelada y que hay fondos suficientes en la cuenta del cliente.

Aquí, la terminal punto de venta envía a la tarjeta un resumen de la transacción (por ejemplo: el importe y la fecha). La tarjeta adjunta sus propios datos, tales como el resultado de la verificación del titular de la tarjeta, y también su contador de transacciones de aplicación (ATC), que es un valor mantenido por la tarjeta, que lleva el conteo del número de transacciones que se han iniciado.

> Posteriormente, la tarjeta responde con un código de autenticación criptográfico, como se indicó, en tratándose de terminales punto de venta es posible que las transacciones se realicen fuera de línea, y el código de autenticación donde se certifica la transacción es almacenado por el terminal para que posteriormente se transmita al emisor (banco). Por su parte, para transacciones en línea, la tarjeta envía un tipo diferente de código de autenticación, un criptograma de solicitud de autorización (ARQC). Este ARQC es enviado al emisor quien responde con un mensaje en el que indica que ese criptograma es válido, al que a su vez incorpora un criptograma de respuesta de autorización (ARPC).
>
> Finalmente, el ARPC se envía a la tarjeta para su verificación, la cual responde con un certificado de transacción (TC) que indica que la transacción ha tenido éxito; o por el otro lado, en cualquier momento puede enviar un criptograma de autenticación de aplicaciones (AAC) rechazando la transacción por no cumplir los requerimientos del propio sistema.

Lo anteriormente reseñado, es un bosquejo de cómo deberían funcionar generalmente la autorización de transacciones efectuadas mediante tarjeta de crédito a través de la digitación de un número de identificación personal en terminal punto venta; sin embargo, el proceso puede variar en atención a los diferentes procedimientos requeridos por la legislación de cada país.

La idea general de este tipo de mecanismos es que los bancos sean capaces de detectar la falsificación de una tarjeta que no contenga las llaves o certificados criptográficos correspondientes, y que la resistencia a la manipulación física del Chip, evitaría que un atacante externo obtuviera la clave[19]; sin embargo, ello no se ha logrado conseguir con las medidas de seguridad existentes hasta el momento.

d) La seguridad en actos de comercio electrónico.

Como ya se precisó, 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.

Por tanto, para atribuir consecuencias de derecho al acto de enviar por correo electrónico un mensaje de datos desde una computadora que realiza una persona a su nombre, es presupuesto o condición indispensable, comprobar que efectivamente fue voluntad de la persona haber enviado el mensaje de datos, es decir, que la persona es el autor de la información generada.[20]

---

[19] Bond Mike, Choudary Omar, Murdoch Steven J., Skorobogatov Sergei y Anderson Ross. (2012). *"Chip and Skim: cloning EMV cards with the pre-play attack"*. Computer Laboratory, University of Cambridge, United Kingdom. Recuperado de: https://www.researchgate.net/publication/230839731_Chip_and_Skim_Cloning_EMV_Cards_with_the_Pre-play_Attack

[20] *Ibídem*, p. 67.

Uno de los ordenamientos fundamentales para el reconocimiento jurídico y legal, tanto del mensaje de datos como de la firma electrónica es la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico, cuyo fin es que los Estados miembros de la Organización de las Naciones Unidas la adopten en sus legislaciones internas para garantizar la seguridad jurídica y la utilización más amplia posible del procesamiento automatizado de datos en el comercio internacional. Entre sus propósitos se encuentra que las legislaciones internas reconozcan la equivalencia funcional entre la información contenida en documentos tangibles (básicamente en papel) y la contenida en documentos intangibles (mensajes de datos generados por medios electrónicos principalmente). [21]

Es decir, se busca que exista la misma confianza entre los documentos tangibles y los intangibles, sin que a aquéllos se les otorgue un valor probatorio diverso por encontrarse en un documento susceptible de tocarse. No obstante, para que ello suceda, se exige que se satisfagan diversos requisitos con el propósito de asegurar que la persona a quien se atribuye el mensaje verdaderamente sea el emisor, de tal suerte que las operaciones o promesas realizadas en mensajes de datos por medios electrónicos tengan la misma validez legal y el mismo reconocimiento por las autoridades que los actos y contratos plasmados en papel tangible como si estuvieran firmados autográficamente.

Para cumplir con sus objetivos la Ley Modelo sigue un nuevo criterio llamado "*del equivalente funcional*", basado en un análisis de las finalidades y funciones del requisito tradicional de la presentación

[21] León Tovar, González García y Vázquez del Mercado Blanco, *op. cit.,* páginas de la 30 a 34.

de un escrito consignado sobre papel con miras a determinar la manera de satisfacer dichas finalidades y funciones con técnicas del comercio electrónico; sin embargo, se reconoce que un mensaje de datos no es por sí mismo el equivalente de un documento en papel, no sólo por su naturaleza distinta sino porque no cumple necesariamente todas las funciones de un documento en papel. En ese sentido, la equivalencia funcional consiste, esencialmente, en atribuirle el mismo valor y eficacia probatoria, a los mensajes y firmas electrónicas, que los que la ley consagra para los instrumentos escritos.

A fin de que esa equivalencia funcional opere, la Ley Modelo exige diversos requisitos que toman en cuenta incluso el grado de fiabilidad, inalterabilidad y facilidad de rastreo que mejor convenga a la función que les haya sido atribuida a los mensajes de datos.

La mencionada equivalencia funcional se manifiesta en tres aspectos de la Ley Modelo sobre Comercio Electrónico aprobada por la Comisión de Naciones Unidas para el Derecho Mercantil Internacional, contenidos en los artículos 5°, 5° bis, 6°, 7° y 8°, mismos que a la letra disponen:

> *"CAPÍTULO II. APLICACIÓN DE LOS REQUISITOS JURÍDICOS A LOS MENSAJES DE DATOS*
>
> ***Artículo 5.*** *— Reconocimiento jurídico de los mensajes de datos*
> *No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.*
>
> ***Artículo 5 bis.*** *— Incorporación por remisión*
> *(En la forma aprobada por la comisión en su 31.° período de sesiones, en junio de 1998)*
> *No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.*

Artículo 6. *— Escrito*

1) Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.

3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 7. *— Firma*

1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma.

3) Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 8. *— Original*

1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:

a) Si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

3) Para los fines del inciso a) del párrafo 1):

a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y

b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.

4) Lo dispuesto en el presente artículo no será aplicable a: [...].". (El subrayado es propio).

Como puede advertirse, la Ley Modelo busca ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitan eliminar algunos de esos obstáculos jurídicos con miras a crear un marco jurídico que permita un desarrollo más seguro del comercio electrónico. En ese sentido, tales preceptos que contienen el criterio de equivalencia funcional fueron introducidos en nuestra legislación en el artículo 93 del Código de Comercio, el cual se transcribe a continuación:

> *"**Artículo 93.-** Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente.*
>
> *Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de Mensaje de Datos, siempre que éste sea atribuible a dichas partes.*
>
> *En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de Mensajes de Datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige."*

En ese sentido, para evitar que se niegue validez jurídica a un mensaje que deba autenticarse por el mero hecho de que no se encuentre en formato característico de los documentos consignados sobre papel, el artículo 7 ofrece una fórmula general cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos si: **a)** se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y **b)** ese método es tan

fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

De esta forma, el Código de Comercio establece que, cuando la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de mensaje de datos, siempre que éste sea atribuible alguna de las partes contratantes.

Con base en ello, bien podría sostenerse que en atención a que se tuvo por cumplido el requisito de verificación del mensaje de datos, pues cuenta con una firma equiparable a la autógrafa por haberse satisfecho el envío de la información necesaria como sería el número de identificación personal (NIP); sin embargo, surge la siguiente interrogante: *¿cómo se puede identificar que la persona que ingresó el NIP es la facultada para ello?*

Para estar en aptitud de responder el cuestionamiento relativo a cómo podría tenerse certeza respecto a que la persona que digita el NIP es diversa al cuentahabiente, debemos hacer referencia a la naturaleza de una de las partes que intervienen en el envío de mensajes de datos, denominado iniciador o emisor.

La Ley Modelo en comento sobre Comercio Electrónico, en su artículo 2º, lo define de la siguiente manera:

> *“c) Por “iniciador” de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él;…”.*

Por su parte, el Código de Comercio define al emisor de la siguiente manera:

> *"Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario...".*

En ese sentido, el iniciador o emisor de un mensaje de datos será la persona que, al amparo de la información enviada, actúa a nombre propio o en cuyo nombre se actúa para generar ese mensaje antes de ser archivado.

Lo cual arroja que, en el caso que se estudia en la presente contradicción de tesis, el iniciador o emisor podría ser la propia persona cuentahabiente que se encuentra facultada para el uso del NIP, o diversa persona que haya sido autorizada por aquélla.

En relación con lo anterior, es preciso señalar que existen reglas para determinar la atribución de los mensajes de datos, es decir, para identificar al emisor. Al respecto, la Ley Modelo en comento sobre Comercio Electrónico establece:

> *"**Artículo 13. —** Atribución de los mensajes de datos*
>
> *1) Un mensaje de datos proviene del iniciador si ha sido enviado por el propio iniciador.*
>
> *2) En las relaciones entre el iniciador y el destinatario, se entenderá que un mensaje de datos proviene del iniciador si ha sido enviado:*
> *a) Por alguna persona facultada para actuar en nombre del iniciador respecto de ese mensaje; o*
> *b) Por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente.*
>
> *3) En las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que un mensaje de*

> *datos proviene del iniciador, y a actuar en consecuencia, cuando:*
> *a) Para comprobar que el mensaje provenía del iniciador, el destinatario haya aplicado adecuadamente un procedimiento aceptado previamente por el iniciador con ese fin; o*
> *b) El mensaje de datos que reciba el destinatario resulte de los actos de una persona cuya relación con el iniciador, o con algún mandatario suyo, le haya dado acceso a algún método utilizado por el iniciador para identificar un mensaje de datos como propio.*
>
> *4) El párrafo 3) no se aplicará:*
> *a) A partir del momento en que el destinatario haya sido informado por el iniciador de que el mensaje de datos no provenía del iniciador y haya dispuesto de un plazo razonable para actuar en consecuencia; o*
> *b) En los casos previstos en el inciso b) del párrafo 3), desde el momento en que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos no provenía del iniciador.*
>
> *5) Siempre que un mensaje de datos provenga del iniciador o que se entienda que proviene de él, o siempre que el destinatario tenga derecho a actuar con arreglo a este supuesto, en las relaciones entre el iniciador y el destinatario, el destinatario tendrá derecho a considerar que el mensaje de datos recibido corresponde al que quería enviar el iniciador, y podrá actuar en consecuencia. El destinatario no gozará de este derecho si sabía, o hubiera sabido de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que la transmisión había dado lugar a algún error en el mensaje de datos recibido.*
>
> *6) El destinatario tendrá derecho a considerar que cada mensaje de datos recibido es un mensaje de datos separado y a actuar en consecuencia, salvo en la medida en que duplique otro mensaje de datos, y que el destinatario sepa, o debiera saber de haber actuado con la debida diligencia o de haber aplicado algún método convenido, que el mensaje de datos era un duplicado.”.*

Por otro lado, de conformidad con lo dispuesto por los artículos 90 y 90 Bis del Código de Comercio, existe presunción *iuris tantum* de que un mensaje de datos ha sido enviado por el emisor o proviene de él, cuando concurran las siguientes circunstancias:

*"**Artículo 90.-** Se presumirá que un Mensaje de Datos proviene del Emisor si ha sido enviado:*

I. Por el propio Emisor;

II. Usando medios de identificación, tales como claves o contraseñas del Emisor o por alguna persona facultada para actuar en nombre del Emisor respecto a ese Mensaje de Datos, o

III. Por un Sistema de Información programado por el Emisor o en su nombre para que opere automáticamente."

*"**Artículo 90 Bis.** Se presume que un Mensaje de Datos ha sido enviado por el Emisor y, por lo tanto, el Destinatario o la Parte que Confía, en su caso, podrá actuar en consecuencia, cuando:*

I. Haya aplicado en forma adecuada el procedimiento acordado previamente con el Emisor, con el fin de establecer que el Mensaje de Datos provenía efectivamente de éste, o

II. El Mensaje de Datos que reciba el Destinatario o la Parte que Confía, resulte de los actos de un Intermediario que le haya dado acceso a algún método utilizado por el Emisor para identificar un Mensaje de Datos como propio.

Lo dispuesto en el presente artículo no se aplicará:

I. A partir del momento en que el Destinatario o la Parte que Confía, haya sido informado por el Emisor de que el Mensaje de Datos no provenía de éste, y haya dispuesto de un plazo razonable para actuar en consecuencia, o

II. A partir del momento en que el Destinatario o la Parte que Confía, tenga conocimiento, o debiere tenerlo, de haber actuado con la debida diligencia o aplicado algún método convenido, que el Mensaje de Datos no provenía del Emisor.

Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del Emisor, se presumirá que se actuó con la debida diligencia si el método que usó el Destinatario o la Parte que Confía cumple con los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas. Cuando se acuerde el uso de comunicaciones electrónicas certificadas, éstas deberán realizarse conforme a los requisitos previstos en la Norma Oficial Mexicana a que se refiere el artículo 49 del Código de Comercio."

Aunque ambas normativas demuestran similitudes sustanciales, debido a que -como se ha explicado- las reformas en la materia del Código de Comercio se desarrollaron con base en la Ley Modelo en comento; sin embargo, no pasa desapercibido para este Alto Tribunal que también existen ciertas diferencias[22], pero ellas resultan atribuibles al error en el traslado de la Ley Modelo a nuestra legislación, sin que lo anterior sea impedimento para resolver, conforme a la instrumentación armónica de ambos ordenamientos, las siguientes interrogantes.

a) ¿Quién o qué puede enviar el mensaje y se entenderá que es el emisor?
b) ¿En qué supuestos el destinatario puede actuar como consecuencia de un mensaje de datos?
c) ¿En cualquier caso si el destinatario aplicó el procedimiento de identificación se entenderá que el mensaje fue enviado por el emisor?

La **primera interrogante** se disipa del análisis de los ordenamientos indicados, específicamente del artículo 90 del Código de Comercio; así como de los párrafos **1)** y **2)** del artículo 13 de la Ley Modelo, de donde derivan las personas o el sistema que puede emitir el mensaje de datos, siendo que estamos en presencia de un emisor, en los siguientes casos:

1. El propio emisor, usando medios de identificación (claves o contraseñas del emisor).
2. Alguna persona facultada para actuar en nombre del emisor, que utilice los medios de identificación.

[22] Ejemplo de lo anterior, son los supuestos de excepción respecto de los cuales los destinatarios de los mensajes de datos pueden actuar en contra del emisor.

3. Por un Sistema de Información programado por el emisor o en su nombre para que opere automáticamente.

De ello se sigue que el emisor de un mensaje de datos puede ser: ***a)*** el propio cuentahabiente, ***b)*** diversa persona autorizada por éste, o ***c)*** un sistema de información automático programado por aquél.

A fin de dar respuesta al **segundo cuestionamiento** –*consistente en determinar en qué supuestos el destinatario puede actuar como consecuencia de un mensaje de datos*-; primeramente debemos señalar que el destinatario, de conformidad con el artículo 89 del Código de Comercio es: "*La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho mensaje"*.

En ese sentido, en el supuesto que nos ocupa, el destinatario será la institución financiera con la cual el usuario firmó el contrato correspondiente para hacer uso de la tarjeta bancaria –ya sea de crédito o débito- para la adquisición de diversos bienes y servicios, mediante la autorización de las transacciones por medio de la firma electrónica.

No pasa desapercibido que el artículo 90 bis del Código de Comercio, así como el párrafo tercero del artículo 13 de la Ley Modelo multicitada, también establecen supuestos con base en los cuales el destinatario puede considerar que el mensaje de datos fue enviado por el emisor, lo que lo faculta para actuar en consecuencia, tales supuestos son los siguientes:

i. Cuando el destinatario haya aplicado en forma adecuada el procedimiento -previamente acordado con el emisor- cuyo fin fuera el de establecer que el mensaje de datos provenía efectivamente del emisor, o

ii. Cuando el destinatario reciba un mensaje de datos resultante de actos de un intermediario -autorizado- que tuviera acceso a algún método utilizado por el emisor para identificar al mensaje de datos como propio.

Tales preceptos establecen una presunción que favorece al destinatario, pues éste podrá actuar para realizar las consecuencias del mensaje de datos siempre y cuando: ***a)*** haya efectuado el procedimiento acordado cuya finalidad haya sido establecer que el mensaje de datos provenía del emisor, o ***b)*** el mensaje proviniera de un intermediario autorizado con acceso a algún método con la misma finalidad referida. Dicho en otras palabras, el destinatario podrá realizar las consecuencias de un mensaje de datos, y éste se entenderá enviado por el emisor -usuario o algún autorizado-, cuando aquél haya aplicado el procedimiento de identificación mencionado.

Sin embargo, los preceptos que se transcribieron también establecen excepciones a esa presunción, lo que da pauta a la resolución de la **tercera interrogante** *-en cualquier caso si el destinatario aplicó el procedimiento de identificación se entenderá que el mensaje fue enviado por el emisor-*.

La respuesta a tal cuestionamiento es negativa, pues los preceptos aludidos establecen claras excepciones a los supuestos referidos respecto a cuándo pueden actuar los destinatarios por consecuencia de un mensaje de datos; a pesar de ello, como

previamente se anticipó, existe una discrepancia entre la normativa nacional y la internacional, pues mientras que la primera establece dos excepciones aplicables, la segunda establece sólo una. Pese a esa diferencia, lo cierto es que la legislación aplicable al caso concreto en principio es el Código de Comercio, por lo que sólo se abordarán las excepciones contenidas en dicha legislación mercantil.

En efecto, la normativa nacional –artículo 90 Bis del Código de Comercio- establece que el destinatario no podrá actuar en consecuencia cuando:

I. El emisor le haya informado que el mensaje de datos no provenía de él, siempre y cuando haya existido un plazo razonable para actuar en consecuencia, o

II. Procediendo con la debida diligencia o aplicando algún método convenido, tenga conocimiento, o debiere tenerlo, que el mensaje de datos no provenía del emisor.

De ello se sigue que, el destinatario no podrá actuar en consecuencia de un mensaje de datos si: ***a)*** el emisor le informó que no emitió el mensaje de datos, siempre y cuando las consecuencias de éste deban realizarse en un plazo razonable, y ***b)*** operó con la debida diligencia o utilizó el método convenido y se da cuenta de que el mensaje de datos no proviene del emisor.

En cuanto a qué debe entenderse por el término “debida diligencia”, el propio precepto 90 bis establece: “*Salvo prueba en contrario y sin perjuicio del uso de cualquier otro método de verificación de la identidad del Emisor, se presumirá que se actuó con la debida diligencia si el método que usó el Destinatario o la Parte que*

Confía cumple con los requisitos establecidos en este Código para la verificación de la fiabilidad de las Firmas Electrónicas".

Con base en lo anterior, es dable concluir que a un mensaje de datos no puede restársele validez jurídica por el simple hecho de ser intangible, sino que cuando la ley requiera que en el acto jurídico conste la firma de una persona, ese requisito se verá colmado si: ***a)*** se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y ***b)*** ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos.

Aunado a ello, se hizo referencia a las personas que pueden ser emisarios de un mensaje de datos, siendo estos: ***a)*** el cuentahabiente, ***b)*** un autorizado o ***c)*** un sistema; y que el destinatario puede actuar en consecuencia de un mensaje de datos cuando: ***i)*** aplicó un procedimiento acordado de identificación del emisor, y ***ii)*** el autorizado utilizó un método acordado para identificar al emisor. Asimismo quedaron explicadas las excepciones previstas en el Código de Comercio, en las cuales se contempla que el destinatario no podrá actuar en consecuencia si: ***1.*** El emisor da aviso de que él no envió el mensaje, y existe un plazo para actuar, y ***2.*** Utilizando un medio de identificación se percata de que la persona que envió el mensaje no era el emisor.

e) La carga probatoria en el Código de Comercio en tratándose de actos autorizados por firma electrónica.

Aun cuando ya se han abordado las presunciones que otorgan derecho al destinatario para poder actuar en consecuencia de un

mensaje de datos entendiéndose que lo formuló el emisor, y que la validez jurídica de una firma electrónica atenderá al método fiable para identificar a la persona firmante; lo cierto es que con ello no puede decidirse de manera tajante a quién otorgarle la carga probatoria en los casos como en el que ahora se estudia, por las consideraciones que se explican a continuación.

Nuevamente, conviene 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”*.

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.

Una vez reseñadas las presunciones legales a favor del destinatario de un mensaje de datos, resulta conveniente transcribir el artículo 1196 del Código de Comercio, que a la letra dispone:

> *“Artículo 1196. También está obligado a probar el que niega, cuando al hacerlo desconoce la presunción legal que tiene a su favor el colitigante”.*

De igual forma, resulta oportuno hacer referencia a lo dispuesto en el artículo 1298-A del mismo ordenamiento legal, el cual se

encuentra inmerso dentro del capítulo denominado *"Del valor de las pruebas"*, y establece lo siguiente:

> *"Artículo 1298-A. Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada.".*

En ese sentido, si la problemática que tuvieron que afrontar los tribunales colegiados contendientes se traduce en que, la parte actora con el carácter de usuario de servicios bancarios, adujo no haber realizado las compras por medio de tarjeta de crédito, por los cuales la institución financiera realizó los cargos y, con base en ello, reclamó la nulidad de los vouchers en los que consta que tecleó su NIP; entonces, en 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, que en este caso fue el uso de la tarjeta bancaria al cual se encuentra integrado un chip con el número de identificación asociado, que una vez tecleado fue verificado por la institución bancaria dando como resultado que en voucher se insertara la leyenda: *"NIP VERIFICADA o PIN VERIFIED".*

Bajo la lógica anterior, sería dable concluir que -como lo establece el artículo 1196 del Código de Comercio-, en este tipo de asuntos el usuario tendría la carga probatoria, pues aunque niega haber digitado el NIP, la institución financiera tiene a su favor la presunción legal contenida en el precepto 90 bis del Código de Comercio. 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.

Pese a ello, debemos 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.

1. La presunción legal a favor del destinatario.

En primer lugar, cabe destacar que la presunción constituye un juicio del legislador o del juez, en virtud del cual se considera como cierto o probable un hecho, con fundamento en las máximas generales de la experiencia, que le indican cuál es el modo normal como suceden las cosas y los hechos.[23]

Así, las presunciones legales son reglas jurídicas sustanciales para la aplicación del derecho objetivo a ciertos casos concretos, cuyos efectos sustanciales se producen fuera del proceso y son reconocidos en éste, donde además influyen en la carga de la prueba.

Pero una vez que el hecho presumido se discute en un proceso, tales presunciones producen el efecto procesal de limitar el presupuesto fáctico que la norma sustancial contempla para que se surtan sus efectos jurídicos, sacando del mismo el hecho presumido, por lo cual el favorecido por ella no necesita demostrarlo, bastándose con probar los otros hechos que sirven de base a tal presunción. Como consecuencia de lo anterior, la parte que niegue el hecho presumido, está sujeta a la carga de probar el hecho contrario. Cabe

[23] Devis Echandia, Hernando, *Teoría general de la prueba judicial,* T. II, 2ª. ed., Editorial P. de Zavalía, Buenos Aires, Argentina, 1972, p. 694.

mencionar que, ese efecto doble de la presunción de origen legal es el que ha descartado a las presunciones como medio probatorios.[24]

Cuando la presunción es creada por el legislador, en tratándose de las *iuris tantum* -como la otorgada a la institución financiera- se considera provisionalmente cierto el hecho mientras no se suministre prueba en contrario. En ese sentido, tales presunciones permiten probar en contrario del hecho presumido.

Sin embargo, 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 esté probado (mientras no se demuestre lo contrario), **en cambio 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 ese sentido, las presunciones legales **iuris tantum** eliminan el hecho presumido del presupuesto fáctico para la producción de los efectos jurídicos perseguidos por quien las invoca e imponen a la otra parte la carga de probar el hecho contrario o la inexistencia del primero[25].

De allí 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**

[24] *Ibídem*, p. 697.
[25] *Ibídem*, p. 701.

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[26], tal como lo establece el artículo 1280 del Código de Comercio, el cual se transcribe:

> *"Artículo 1280. El que tiene a su favor una presunción legal, sólo está obligado a probar el hecho en que se funda la presunción".*

Motivo por el cual, 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.

2. Los supuestos que podrían originar asuntos como los abordados en los ejecutorias contendientes.

[26] Al respecto Velandia sostiene que: *"El detalle de la falta de firma de los documentos informáticos no implica que carezcan de valor probatorio. Lo que se requiere es que los jueces cuenten con suficiente referencia probatorias confiables, al extremo de que le produzcan una certeza razonable sobre la existencia del hecho controvertido a establecer, para que se obtenga la debida seguridad sobre el documento electrónico. […] es claro que la prueba del documento electrónico puede requerir de la complementación de varios medios probatorios para que el juez pueda llegar a la convicción de la verdad procesal, como pueden ser las experticias, reproducciones, testimonios, la confesión o los medios complementarios que deben ser valorados según su tipología… y también puede plantearse la prueba científica que requiere de informes periciales con soportes electrónicos cuya valoración amerita la observancia de aspectos técnicos o científicos que el juez no tiene que conocer directamente"*. Véase Velandia Ponce, Rómulo. "El documento electrónico y sus dificultades probatorias". Alvaronora, Venezuela, 1ª ed. 1995, págs. 86 y 87.

Ahora bien, antes de arribar a una conclusión con base en las presunciones otorgadas a favor de la institución financiera -destinatario- y la carga de la prueba establecida al usuario, resulta conveniente hacer alusión a los supuestos que dieron origen a las circunstancias fácticas en las ejecutorias contendientes.

Como ya se mencionó a lo largo de la presente ejecutoria, los usuarios del servicio bancario adujeron no haber efectuado diversas compras realizadas físicamente en un establecimiento comercial, en las cuales se utilizó como medio de pago su tarjeta bancaria la cual cuenta con chip, verificándose las compras por medio de la digitación del número de identificación personal, y respecto de las cuales se expidió el voucher correspondiente en el que se observa la leyenda: *“NIP VERIFICADA o PIN VERIFIED”*.

Los usuarios argumentaron que otra persona acudió a efectuar las compras a los diversos comercios, utilizando como medio de pago su tarjeta bancaria, digitando su NIP.

Al respecto, debe indicarse que resulta lógico que una persona utilizara la tarjeta bancaria y NIP de otro individuo para realizar los cargos a su cuenta, lo que se puede advertir cotidianamente en un sinfín de actos, donde el tarjetahabiente otorga autorización para la utilización de su tarjeta y NIP a una persona de su entera confianza para realizar compras en establecimientos en los cuales ni siquiera se requiere a la persona una identificación para comprobar que efectivamente la persona física es la titular de la tarjeta en la que se encuentra el nombre del tarjetahabiente. Otro ejemplo de lo anterior, se suscita cuando por parte de la institución bancaria se entregan tarjetas provisionales que ni siquiera están personalizadas, en ese

supuesto la persona que actúe sobre aquélla ni siquiera podría verificar la identidad; máxime que en cualquiera de los dos supuestos, la compraventa e identidad del emisor se corrobora con la digitación del NIP, como se ha explicado.

En tales supuestos, merece especial atención que de acuerdo con el artículo 90[27] en concatenación el diverso 99, ambos del Código de Comercio[28], el destinatario será responsable de las obligaciones firmadas a su cuenta; no obstante, lo que adujeron los cuentahabientes actores fue que una persona no autorizada por ellos, fue que hizo uso de su tarjeta bancara y NIP para efectuar las transacciones.

Derivado de lo anterior, es claro que los datos tanto de las tarjetas de crédito como del número de identificación personal, pueden obtenerse de manera fraudulenta para realizar compras presenciales; para lo que debemos tener presente las diferentes formas en que

---

[27] *"**Artículo 90.** Se presumirá que un Mensaje de Datos proviene del Emisor si ha sido enviado:*
I. Por el propio Emisor;
II. Usando medios de identificación, tales como claves o contraseñas del Emisor o por alguna persona facultada para actuar en nombre del Emisor respecto a ese Mensaje de Datos, o
III. Por un Sistema de Información programado por el Emisor o en su nombre para que opere automáticamente".

[28] *"**Art. 99.** El Firmante deberá:*
I. Cumplir las obligaciones derivadas del uso de la Firma Electrónica;
II. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma;
III. Cuando se emplee un Certificado en relación con una Firma Electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el Certificado, con su vigencia, o que hayan sido consignadas en el mismo, son exactas.
El Firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en el presente artículo, y
IV. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia.".

actúan las personas para cometer fraudes bancarios[29], entre las más frecuentes y más fáciles de utilizar se encuentran las siguientes:

- **El "skimming".** Es un dispositivo electrónico que realiza una copia de la banda magnética de la tarjeta, y a través de una computadora pasan los datos de aquélla a una tarjeta vacía.

- **Métodos para capturar el NIP[30].**
  - **La cámara estenopeica**, método que consiste en instalarla cerca del cajero automático, la cual graba en video al tarjetahabiente mientras ingresa su NIP.
  - **Teclado de NIP falso**, el cual se coloca sobre el teclado legítimo en el cual el usuario digitará su NIP.

- **Gratificaciones falsas.** Opera cuando te avisan que has sido ganador de un premio, ya sea un viaje o cantidad de dinero, pero el único requisito que te ponen es proporcionar tus datos financieros.

- **Phishing.** En ese método se comunican con el usuario para informarle que existen problemas con algún producto o servicio financiero con el que cuenta, y piden verificar el tipo de problema.

- **"Las palomas".** El defraudador adquiere una USB o memoria extraíble con información de usuarios de cualquier institución financiera. Posteriormente, con la ayuda de una

[29] Gutiérrez, Noé, 2016, "Clonación e tarjeta, acciones para prevenir y cuidar tus finanzas", Revista Proteja su dinero, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, núm. 195, junio, páginas 10-13.
[30] Rivero Mario y Gottschalk Franz, "Los Ataques de Skimming en Cajeros Automáticos y cómo Prevenirlos". Disponible en el sitio electrónico: *https://usa.visa.com/dam/VCOM/download/merchants/Webinar-Preventing-ATM-Skimming-Spanish-021914.pdf*. Fecha de consulta: trece de noviembre de dos mil dieciocho.

computadora, descarga dicha información a una tarjeta en blanco llamada “paloma”; sin embargo, dicha tarjeta no cuenta con una banda magnética, ni logotipos de alguna institución financiera, sino que solo cuenta con un chip electrónico. Una vez que tiene la tarjeta con toda la información del usuario, acude a diversos comercios para realizar cualquier tipo de operación para que al momento de ingresar la tarjeta pueda disponer de efectivo. Para que el delincuente pueda tener el dinero en sus manos, anteriormente tuvo que relacionarse con la persona del lugar donde cree que podrá realizar el fraude y en cambio le ofrece una gratificación.

- **Ofertas en servicios no solicitados.** Sucede cuando empresas “piratas” ofrecen viajes o autos sólo con demostrar que una persona es tarjetahabiente o depositar alguna cantidad de dinero, y para ello peticionan información del usuario acreditado.

- **Robo de tarjeta.** Este supuesto no necesita mayor explicación, pues es aquél en el cual una persona con ánimo de dominio y sin consentimiento de quien legalmente pueda otorgarlo, se apodera de la tarjeta.

- **Secuestro exprés.** De conformidad con el artículo 163 Bis del Código Penal para la Ciudad de México, comete el delito de privación de la libertad en su modalidad de secuestro exprés, el que prive de la libertad a otro por el tiempo estrictamente indispensable para cometer los delitos de robo o extorsión, o para obtener algún beneficio económico. En ese sentido, cabe la posibilidad de que una persona prive de su libertad a otra, con la finalidad de obligarla a realizar

diversos actos con su tarjeta bancaria, digitando su NIP para el beneficio del delincuente.

Como previamente se indicó, ante la facilidad de clonación que implicaban las tarjetas bancarias que sólo contaban con banda magnética aunado al avance tecnológico, se comenzó a implantar el chip en los plásticos, lo cual se hizo paulatinamente en México desde el año dos mil diez[31].

Si bien en un primer momento se creía que era imposible la clonación de tarjetas con chip, lo cierto es que conforme se fueron introduciendo a la esfera comercial, los defraudadores idearon mecanismos para que tal sistema de seguridad fuera tan vulnerable como en su momento lo fue la simple banda magnética, tan es así que ya han sido diversos casos a nivel mundial[32], y en México la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros recientemente, el seis de septiembre de dos mil dieciocho emitió un comunicado[33] en el que hizo saber un nuevo mecanismo de fraude que permite clonar los datos de las tarjetas de chip, así como el NIP.

---

[31] La implementación del chip en tarjetas bancarias se realizó a partir de las modificaciones a las Disposiciones de carácter general aplicables a las Instituciones de Crédito, publicadas en el Diario Oficial de la Federación el veintisiete de enero de dos mil diez.

[32] Thompson, T. *Hay un problema relacionado con las nuevas tarjetas con chip*. AARP, disponible en el sitio electrónico: https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2018/muchos-comercios-sin-sistema-para-tarjeta-de-credito-con-chip.html. *Chip en tarjeta, bueno pero no infalible*, 22 de julio de 2013, Expansión, disponible en el sitio electrónico: *https://expansion.mx/economia/2013/07/22/chips-en-tarjetas-dificultan-clonacion*. Ortega, Javier, El chip limita la clonación de tarjetas, El Comercio, disponible en el sitio electrónico: *https://www.elcomercio.com/actualidad/seguridad/chip-limita-clonacion-de-tarjetas.html.* Fecha de consulta de los tres artículos: trece de octubre de dos mil dieciocho.

[33] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, *Alerta CONDUSEF ante nuevos mecanismos de fraudes en terminales puntos de venta,* 6 de septiembre de 2018, disponible en el sitio electrónico: *https://www.gob.mx/condusef/prensa/alerta-condusef-ante-nuevos-mecanismos-de-fraudes-en-terminales-puntos-de-venta?idiom=es*, fecha de consulta de los tres artículos: trece de octubre de dos mil dieciocho.

En tal comunicado, la Comisión informó que recibió una *"Notificación Morada"* de la Interpol, a fin de alertar a los comercios que utilicen terminales punto de venta ante la instalación de malware que permite clonar los datos de las tarjetas de crédito o de débito de chip y NIP, y que de acuerdo con la notificación, el *modus operandi* aplicado comienza cuando los presuntos estafadores, haciéndose pasar por personal de las instituciones financieras, envían mensajes aparentemente auténticos a las empresas o pequeños comercios informándoles de una *"actualización del sistema de la terminal punto de venta"* (del ordenador, no del lector de tarjetas físico), para lo cual les solicitan acceso remoto a la terminal, infectando la máquina a distancia.

Una vez instalado el malware, los intrusos pueden ver las transacciones efectuadas con tarjetas, interceptarlas, capturar la información e incluso redirigir los datos de las tarjetas a un servidor externo, sin que el comercio dueño de la terminal punto de venta o el tarjetahabiente se den cuenta, de tal forma que pueden conseguir los siguientes datos:

- Número de cuenta del cliente
- Número de tarjeta
- Fecha de vencimiento
- Tipo de tarjeta
- Otros datos del titular de la tarjeta

Estos datos son cargados a una tarjeta conocida como *"Tarjeta Paloma"* -como la anteriormente explicada- y toda vez que el malware permite manipular el proceso de verificación de la autenticidad del titular de la tarjeta, cualquier número puede ser considerado válido con

NIP, pudiendo ser utilizada para realizar cualquier tipo de compra, ya sea en terminales punto de venta o compras en línea.

Este tipo de mecanismos resultan más complejos para su implementación, precisamente por la tecnología y técnicas invertidas para la obtención de información sustraída tanto de los propios Chips de las tarjetas bancarias, como de las terminales punto de venta; empero de igual forma resultan efectivos. Algunos otros ejemplos de estos mecanismos son:

- **El “fuzzing".** Es una técnica donde se utiliza un proceso automatizado para descubrir vulnerabilidades en la seguridad de la tarjeta. Esto no requiere ningún conocimiento del software que se está probando y ha sido ampliamente utilizado en otros contextos, tanto por los investigadores de seguridad, como por criminales, y es una técnica muy efectiva.

  Guyot ilustra el uso de fuzzing en *applets* (*Un applet es un componente de una aplicación que se ejecuta en el contexto de otro programa, por ejemplo, en un navegador web. El applet debe ejecutarse en un contenedor, que le proporciona un programa anfitrión, mediante un plugin, o en aplicaciones como teléfonos móviles que soportan el modelo de programación por "applets"*), donde demuestra lo fácil que es determinar con precisión los comandos (es decir, los códigos de instrucciones) que son aceptados por una aplicación. Los comandos, también llamados Application DataUnits (APDU), se codifican de acuerdo con la norma ISO 7816. Un comando que se reconoce induce una acción y el

retorno de datos o de palabras de estado que indican un error interno[34]. Así, un *applet* hostil es cualquiera que, cuando se descarga, intenta monopolizar o explotar los recursos de su sistema de una manera inapropiada. Un *applet* que realiza, o hace que alguien realice, una acción que de otra manera no realizaría, debe considerarse hostil, ejemplo de esto son los *applets* de denegación de servicio, los de falsificación de correo o los que ejecutan subrepticiamente el programa de otras personas en su estación de trabajo.[35]

- **Ataques invasivos, semi-invasivos o no invasivos.** Un enfoque adicional para comprometer la seguridad de la tarjeta es atacar el Chip en sí mismo, en lugar de comprometer el software. Lo anterior se logra mediante un conjunto de técnicas conocidas como ataques invasivos y semi-invasivos, donde el Chip se retira de la tarjeta y es manipulado utilizando equipos de laboratorio. Estas técnicas pueden descubrir información confidencial o crear fallos cuidadosamente elegidos en la aplicación de restricciones de seguridad. Por su parte, los ataques no invasivos también son posibles, y en ellos no se requiere la remoción del chip de la tarjeta[36]. Un ejemplo de este último supuesto lo encontramos al medir las variaciones en el consumo de energía por minuto de las tarjetas inteligentes, de esta manera es posible extraer claves criptográficas; aunque cabe aclarar que las tarjetas

[34] Citado por Alimi V., Vernois S. y Rosnberger C. Analysis of Embedded Aplications by Evolutionary Fuzzing. Normandie, Univ, France. (Vincent Guyot. “Smart card, the invisible wallet”. In Proceedings of the 9th European Conference on Information Warfare and Security, 2010). Recuperado de: https://www.researchgate.net/publication/263273041_Analysis_of_Embedded_Applications_By_Evolutionary_Fuzzing.
[35] LaDue Mark D. “Hostile Applets on the Horizon” (1996). Recuperado de: https://www.cis.upenn.edu/~bcpierce/courses/629/papers/LaDue-Hostile.html
[36] Murdoch Steven J. *Op. Cit*. P.101.

comúnmente incorporan defensas contra este tipo de ataques, aunque no se ha documentado que sean siempre efectivos.[37]

- **El "relay attack" (ataque de relevo)**. Otros ataques contra el Chip y NIP no requieren la explotación de las vulnerabilidades de seguridad en absoluto, pero se basan en detonar las limitaciones inherentes de las tarjetas. Uno de estos enfoques es el "ataque de relevo", que hace uso del hecho de que las tarjetas inteligentes no tienen una pantalla para informar al titular de la tarjeta qué transacción están autorizando.

  El ataque funciona de la siguiente manera: el titular de la tarjeta inserta su tarjeta auténtica en una terminal de punto de venta con mecanismo Chip y NIP comprometido, y aproximadamente al mismo tiempo, el criminal inserta una tarjeta de relevo especial en una terminal real de Chip que pida autorización mediante NIP. Cuando la tarjeta de relevo es interrogada, pasa varios mensajes desde y hacia la tarjeta auténtica a través de la terminal comprometida[38]. Así, la terminal real creerá que la tarjeta de relevo es auténtica y de esta forma el cliente piensa que está autorizando una transacción específica, pero en realidad el defraudador está llevando a cabo uno mucho más grande, potencialmente del otro lado del mundo.[39]

---

[37] *Ibídem*.

[38] Drimer Sam y Murdoch Steven J. "Keep your enemies close: Distance bounding against smartcard relay attacks". University of Cambridge, Computer Laboratory, UK. Recuperado del sitio: http://www.cse.uconn.edu/~akiayias/cse281sp08/CSE281_Computer_Security/Reading_files/Drimer-Murdoch.pdf

[39] Este tipo de casos ha sido documentado, como se advierte del artículo "Now Banks are trying to pin the blame for card fraud on you". Bringnall, Miles. The Guardian. UK. Mayo 2012, que textualmente dispone: *"Even in the face of overwhelming evidence that the account holder was miles away at the time, and it could not have been them, some banks*

- **Errores en la personalización.** Puede incluso que ni siquiera sea necesario comprometer la tarjeta del cliente. Lo anterior en virtud de que, para clonar una tarjeta bancaria, se necesita información específica, misma que está disponible en la oficina de personalización (donde las tarjetas en blanco tienen las claves y datos del cliente precargados), y en el centro de autorización (donde se envían los mensajes de la autorización de transacción). Tanto la personalización, como la autorización de la tarjeta bancaria se realiza por parte del banco emisor, pero esa labor es comúnmente subcontratada (aun cuando sea de forma parcial) en prestadores de servicios especializados.

  De esta forma, si un criminal es capaz de interferir o extraer información de cualquiera de estos procesos, podrían crear una tarjeta clonada sin haber visto incluso el plástico verdadero.

  Otro ejemplo sería el caso en que se enviara una tarjeta duplicada con datos de un solo usuario a domicilios diferentes, lo que en sí mismo conllevaría un gran riesgo de seguridad para el usuario. En tratándose de transacciones en disputa, los bancos comúnmente suponen que exactamente una copia de cada tarjeta se ha producido; por lo tanto, si los registros del banco muestran que la autorización de transacción ha tenido éxito, infiere que la tarjeta en particular se emitió al cliente y considera que éste ha sido negligente al permitir el uso indebido de su tarjeta sin autorización, haciéndolo responsable por la transacción; sin embargo, el supuesto de que las

---

have been insisting their customer is liable". Recuperado de: https://www.theguardian.com/money/2012/may/04/banks-pin-card-fraud

> tarjetas clonadas no pueden existir resulta inválida, ante la clara evidencia de las vulnerabilidades de seguridad anteriormente reseñadas.[40]

Lo anterior, hace patente la viabilidad de que una persona se presente físicamente a un comercio con datos del usuario –tarjeta bancaria con chip y su NIP- para efectuar alguna compraventa o el pago de un servicio –lo que en sí mismo pone en entredicho la vulnerabilidad del sistema operativo de los servicios bancarios mediante la autorización de firma electrónica en las terminales punto de venta-; siendo que el resultado de digitar el número de identificación personal, dará como consecuencia la verificación satisfactoria de la transacción, lo que se traduce en el correspondiente cargo a la cuenta del tarjetahabiente.

Por ende, la presunción aludida en el sentido de 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 dispositivos Chip o el número de identificación personal, por lo que en el supuesto en el que el usuario niegue haber efectuado esos cargos al no haber digitado su NIP; la institución bancaria 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 de creación del mensaje de datos; máxime si se considera que en los casos de transacciones en disputa el emisor normalmente dispone de casi toda la evidencia que se presenta ante el tribunal.[41]

---

[40] Murdoch Steven J. *Op. Cit.*

[41] Al respecto, debe considerarse lo que sostienen Bond, Choudary, Murdoch, Skorobogatov y Anderson, en su obra “Chip and Skim”, anteriormente citada, donde

Además, las alegaciones de los bancos en el sentido de que un cliente ha actuado de manera fraudulenta o que ha sido negligente con la información personal que le proporcionó el emisor, no encuentran sustento, en atención a que claramente está en sus intereses el sugerir esa explicación con preferencia a la clonación o defraudación de sus sistemas, porque de esa manera están en posibilidad de transferir la pérdida al cliente, mientras que la clonación deja la pérdida en manos de la institución bancaria.[42]

Cabe destacar que uno de los dilemas que pueden presentarse con el traslado de la carga probatoria a favor del usuario, es que éste tendría que comprobar un hecho negativo consistente en que a) no fue él quien digitó el número de identificación personal o que b) no estaba presente en ese momento. En el primer supuesto, como se indicó, el consumidor se encuentra en una posición de desventaja, primero porque previamente al juicio deben iniciar un procedimiento interno de resolución de conflictos ante el banco para el reconocimiento y devolución de los cargos, y posteriormente, porque durante el contencioso no cuenta con los mecanismos tecnológicos necesarios a los que sí puede acceder la institución bancaria. El segundo caso es

---

sostienen fehacientemente que los bancos que destruyen la evidencia deben de ser automáticamente responsables del pago de la totalidad de las cantidades en disputa, incluyendo costos; **PERO SOBRE TODO, LA CARGA DE LA PRUEBA DEBE RECAER EN LOS BANCOS** y no en los consumidores tal como lo ha reconocido la Asociación para servicios de compensación de pagos del Reino Unido…". El texto original es el siguiente: "*Banks which destroy evidence should become automatically liable for the full sums in dispute, including costs.* ***ABOVE ALL, THE BURDEN OF PROOF MUST LIE ON THE BANKS, NOT THE CUSTOMER****. The Payment Services Directive already requires this…"*.

[42] Al respecto, Pat Hurley en su carácter de ombudsman financiero del Reino Unido, nos explica que: *"Debemos recordar que a medida que los servicios financieros cambian y las estafas evolucionan con él, lo que se considera un comportamiento negligente también cambiará inevitablemente, puesto que la creciente sofisticación de las estafas significa que la barrera para la negligencia grave aumentará, no se trata solo de demostrar que alguien ha sido descuidado con sus datos financieros personales* -como el NIP-, *es por ello que el desafío para el sector de servicios financieros y sus reguladores, cuando deciden acerca de lo justo y razonable, deben asegurarse de que se refleje lo que es esencialmente una situación en constante cambio"*. Financial Ombudsman Service. Ombudsman news, número 145, Agosto 2018. Recuperado de: https://www.financial-ombudsman.org.uk/publications/ombudsman-news/145/145-ombudsman-focus-fraud-and-scams.html

igual de complicado, en atención a que para acreditar que no estaba físicamente presente en el momento de la transacción, el usuario debe recurrir a la obtención de pruebas en poder de terceros, como serían por ejemplo las imágenes y videos obtenidas por circuito cerrado de televisión (CCTV) o cámaras de seguridad. La problemática suscitada en ese supuesto es que, al reportar una transacción fraudulenta a la institución bancaria, al cliente se le devuelve inmediatamente el monto de la operación hasta en tanto no se lleve a cabo la investigación interna (la cual puede llevar semanas), de esta manera el cliente queda satisfecho momentáneamente con el resultado; no obstante, si la investigación resulta desfavorable para el cliente, se revierte el reembolso de la cuenta. Es a partir de este punto, cuando el cliente estará motivado para obtener la evidencia indicada del registro de terceros, pero la lógica indica que en esta etapa los registros ya pueden haber sido eliminados; e incluso, con independencia de que pudieran existir, los propietarios del comercio no estarían obligados a responder favorablemente a la entrega de la solicitud de las videograbaciones, máxime si tomamos en cuenta que en la actualidad estas nuevas realidades han suscitado que los comerciantes y los bancos generen actitudes hostiles en el sistema de pago, gracias a los cargos por transacciones de sobrepago y las devoluciones de cargo.[43]

Finalmente, en un acercamiento al derecho comparado, cabe destacar que, con respecto a los sistemas bancarios, el organismo representativo de la industria bancaria del Reino Unido (APACS), en su política de administración del NIP, establece: *“El proceso de administración de NIP no solo debe ser seguro, sino que también debe ser demostrablemente seguro. Si la seguridad del NIP es cuestionada*

[43] Bond Mike, Choudary Omar, Murdoch Steven J., Skorobogatov Sergei y Anderson Ross. *Op. Cit*. P. 1.

públicamente, ya sea en los medios o en un tribunal de justicia, debe ser posible responder a tal desafío, avalando la respuesta con evidencia. Además, el uso de ese evidencia en el dominio público no debe en sí misma comprometer la seguridad"[44]. Asimismo, no debe perderse de vista que en el año dos mil dos (2002), dicha institución reconoció que la introducción de los NIP's cambió la responsabilidad de identificar al titular de la tarjeta, dejando a la tecnología como medio fundamental de confiabilidad, misma que sería suficientemente fiable o rentable para cumplir los requisitos de la industria de tarjetas del Reino Unido a mediano plazo (aproximadamente diez años). Sin embargo, también reconoció la existencia de mecanismos alternativos como medidas adicionales de seguridad, por ejemplo poner fotografías de identificación o la incorporación de escaneo de detalles biométricos (huella, iris ocular y el reconocimiento de voz) en las tarjetas bancarias. Tales mecanismos no fueron adoptados por las instituciones financieras, al considerar que no existían elementos para determinar su confiabilidad, y sobre todo por el costo/beneficio de la implementación.[45]

f) Conclusión.

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; no

---

[44] Mason, Stephen. "When bank systems fail. Debit cards, credit cards, ATM's, mobile and online banking: your rights and what to do when things go wrong". London: PP Publishing. 2014. El texto original de la párrafo transcrito, es el siguiente: *"The **PIN Administration process must not only be secure, but also be demonstrably secure**. **If PIN Security is publicly challenged, either in the media or in a court of law, it must be possible to respond to such a challenge and for the response to be supported with evidence.** Furthermore, the use of that evidence in the public domain must not in itself compromise security."*

[45] Association for Payment Clearing Services (APACS). "Card Fraud. The Facts 2002." APACS Plastic Fraud Prevention Forum (PFPF). London, UK. Abril 2002. Recuperado de: "http://www.dematerialisedid.com/PDFs/cardfraudfacts20021.pdf"

> obstante, a la par de los avances técnicos, también se ha acrecentado el uso ocasional malintencionado de recursos similares para burlarlos.

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.[46]

Con base en las premisas reseñadas se concluye que si bien, de conformidad con el artículo 1196 del Código de Comercio la carga de la prueba corresponde a quien niega cuando existe una presunción legal a favor de su colitigante, siendo que en ese caso el artículo 90 bis del Código de Comercio prevé diversas presunciones a favor de la institución financiera; lo cierto es que el hecho del cual se presume aquél y que le sirve de antecedente, sí necesita de mayores elementos probatorios para que el juez lo considere cierto y pueda aplicar esa presunción.

Por ende, 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

[46] Bond, Mike. *Op. Cit*.

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:

1. Haya efectuado el procedimiento acordado cuya finalidad haya sido establecer que el mensaje de datos provenía del emisor, o
2. El mensaje proviniera de un intermediario autorizado con acceso a algún método con la misma finalidad referida.

Por tanto, si la institución financiera quiere gozar de la presunción legal referente a tener como emisor al que envió el mensaje 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.[47]

En ese sentido, 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

[47] Nuevamente vale la pena recalcar que, en este tipo de asuntos no se cuestiona la 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.

carácter general aplicables a las Instituciones de Crédito[48], 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 autentificación a que se refiere el artículo 310[49], los cuales pueden ser categoría 2, 3 o 4, cuando se pretenda el pago de bienes.

---

[48] "**Artículo 313.-** Las Instituciones deberán solicitar a sus Usuarios, para la celebración de operaciones o prestación de servicios a través de Medios Electrónicos, un segundo Factor de Autenticación de las Categorías 3 o 4 a que se refiere el Artículo 310 de estas disposiciones, adicional al utilizado, en su caso, para iniciar la Sesión y en cada ocasión en que se pretenda realizar cada una de las operaciones y servicios siguientes:
I. Transferencias de recursos dinerarios a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y de bienes o servicios, así como las autorizaciones e instrucciones de domiciliación de pago de bienes o servicios;…".

[49] "**Artículo 310.-** 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. Dichos Factores de Autenticación, dependiendo del Medio Electrónico de que se trate y de lo establecido en las presentes disposiciones, deberán ser de cualquiera de las categorías siguientes:
I. **Factor de Autenticación Categoría 1**: Se compone de información obtenida mediante la aplicación de cuestionarios al Usuario, por parte de operadores telefónicos o remotos, en los cuales se requieran datos que el Usuario conozca. En ningún caso los Factores de Autenticación de esta categoría podrán componerse únicamente de datos que hayan sido incluidos en comunicaciones impresas o electrónicas enviadas por las Instituciones a sus clientes.
Instituciones, en la utilización de los Factores de Autenticación de esta categoría, para verificar la identidad de sus Usuarios, deberán observar lo siguiente:
a) Definir previamente los cuestionarios que serán practicados por los operadores telefónicos o remotos, impidiendo que sean utilizados de forma discrecional, y
b) Validar al menos una de las respuestas proporcionadas por sus Usuarios, a través de herramientas informáticas, sin que el operador pueda consultar o conocer anticipadamente los datos de Autenticación de los Usuarios.
II. **Factor de Autenticación Categoría 2**: Se compone de información que solo el Usuario conozca e ingrese a través de un Dispositivo de Acceso, tales como Contraseñas y Números de Identificación Personal (NIP), y deberán cumplir con las características siguientes:
a) En ningún caso se podrá utilizar como tales, la información siguiente:
i El Identificador de Usuario.
ii El nombre de la Institución.
iii Más de tres caracteres idénticos en forma consecutiva.
iv. Más de tres caracteres consecutivos numéricos o alfabéticos.
No resultará aplicable lo previsto en el presente inciso para el caso de Pago Móvil, Banca Móvil y las operaciones realizadas a través de Cajeros Automáticos y Terminales punto de Venta, siempre que las Instituciones informen al Usuario al momento de la contratación, de la importancia de la composición de las Contraseñas para estos servicios.
b) Su longitud deberá ser de al menos seis caracteres, salvo por los servicios ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta, en cuyo caso será de al menos cuatro caracteres.
i Derogado.
ii Derogado.
iii Derogado.

c) La composición de estos Factores de Autenticación podrá incluir caracteres numéricos, alfabéticos u otros, cuando el Dispositivo de Acceso lo permita.
Las Instituciones deberán permitir al Usuario cambiar sus Contraseñas, Números de Identificación Personal (NIP) y otra información de Autenticación estática, cuando este último así lo requiera, utilizando los servicios de Banca Electrónica.
Tratándose de Contraseñas o Números de Identificación Personal (NIP) definidos o generados por las Instituciones durante la contratación de un servicio de Banca Electrónica o durante el restablecimiento de dichas contraseñas, las propias Instituciones deberán prever mecanismos y procedimientos por medio de los cuales el Usuario deba modificarlos inmediatamente después de iniciar la Sesión correspondiente. Las Instituciones deberán contar con controles que les permitan validar que las nuevas Contraseñas o Números de Identificación Personal (NIP) utilizadas por sus Usuarios, sean diferentes a los definidos o generados por las propias Instituciones.
Las Instituciones deberán recomendar a sus Usuarios en el proceso de contratación del servicio de Banca Electrónica, que mantengan Contraseñas seguras.
III. **Factor de Autenticación Categoría 3**: Se compone de información contenida o generada por medios o dispositivos electrónicos, así como la obtenida por dispositivos generadores de Contraseñas dinámicas de un solo uso. Dichos medios o dispositivos deberán ser proporcionados por las Instituciones a sus Usuarios y la información contenida o generada por ellos, deberá cumplir con las características siguientes:
a) Contar con propiedades que impidan su duplicación o alteración.
b) Ser información dinámica que no podrá ser utilizada en más de una ocasión.
c) Tener una vigencia que no podrá exceder de dos minutos.
d) No ser conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes o comisionistas de la Institución o por terceros.
Las Instituciones podrán proporcionar a sus Usuarios medios o dispositivos que generen Contraseñas dinámicas de un solo uso, las cuales utilicen información de la Cuenta Destino y en el caso de operaciones no monetarias, cualquier otra información relacionada con el tipo de operación o servicio de que se trate, de manera que dicha Contraseña únicamente pueda ser utilizada para la operación solicitada. En estos casos, no será aplicable lo dispuesto en el inciso c) de la presente fracción, así como lo establecido en el cuarto párrafo del Artículo 314 de estas disposiciones en relación al tiempo en que deberán quedar habilitadas las Cuentas Destino.
Asimismo, las Instituciones podrán considerar dentro de esta categoría a la información contenida en el circuito o chip de las Tarjetas Bancarias con Circuito Integrado, siempre y cuando dichas tarjetas se utilicen únicamente para operaciones que se realicen a través de
Cajeros Automáticos y Terminales Punto de Venta y tales Dispositivos de Acceso obtengan la información de la tarjeta a través del dicho circuito o chip.
Las Instituciones que aprueben la celebración de operaciones mediante el uso de tarjetas bancarias sin circuito integrado, en Cajeros Automáticos y Terminales Punto de Venta, deberán pactar con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en el uso de dichas tarjetas. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.
Tratándose de Banca Host to Host, las Instituciones podrán utilizar como Factor de Autenticación de esta Categoría, cualquier mecanismo que les permita verificar que los equipos de cómputo o dispositivos utilizados por los Usuarios para establecer la comunicación, son los que la propia Institución autorizó.
Las Instituciones podrán utilizar tablas aleatorias de Contraseñas como Factor de Autenticación de esta Categoría, siempre y cuando dichas tablas cumplan con las características listadas en los incisos a), b) y d) de la presente fracción. Para el caso del inciso a), las Instituciones deberán asegurarse que las propiedades que impidan la duplicación o alteración se cumplan hasta el momento de la entrega al Usuario. En todo caso, las Instituciones deberán obtener la previa autorización de la Comisión, en cuya solicitud deberán exponer los controles que les permitirán a los Usuarios realizar operaciones de forma segura.

Tales factores de autentificación son: ***a)*** Categoría 2: Puede constituirlo un NIP, ***b)*** Categoría 3: Puede constituirlo una tarjeta con chip, y ***c)*** Categoría 4: Se compone de información del usuario derivada de sus propias características físicas.

Por ende, 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 -siendo que el artículo 1298-A del Código de Comercio señala que el destinatario de la información es quien debe probar la fiabilidad del método que utilizó para la creación de la

---

Las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán pactar con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones no reconocidas por aquellos realizadas a través del servicio de Banca Electrónica de que se trate. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.

IV. **Factor de Autenticación Categoría 4**: Se compone de 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. Previo a la captura de los datos biométricos mencionados de sus Usuarios, las Instituciones deberán capturar los mismos datos biométricos de sus empleados, directivos y funcionarios encargados de esta función, y verificar que los datos biométricos de clientes no correspondan con los de dichos empleados, directivos y funcionarios. Tratándose de la captura de huellas dactilares e identificación facial que las Instituciones pretendan mantener en sus bases de datos para efectos de autenticación de sus clientes, empleados, directivos y funcionarios, estas deberán sujetarse a los requerimientos técnicos que se establecen en el Anexo 71 de las presentes disposiciones.

Tratándose de huellas dactilares, será necesario que, para conformar las bases de datos a que se refiere el párrafo anterior y poderlas usar con posterioridad para efectos de autenticación, las Instituciones den de alta a sus clientes, empleados, directivos y funcionarios previa autenticación de sus huellas con el Instituto Nacional Electoral.

Las Instituciones que utilicen los Factores de Autenticación de esta categoría, deberán aplicar para cada operación a la información de Autenticación obtenida por dispositivos biométricos, elementos que aseguren que dicha información sea distinta cada vez que sea generada, a fin de constituir Contraseñas de un solo uso, que en ningún caso puedan utilizarse nuevamente o duplicarse con la de otro Usuario.

Las Instituciones podrán considerar dentro de esta categoría la firma autógrafa de sus Usuarios en los comprobantes generados por las Terminales Punto de Venta o bien la plasmada en dispositivos ópticos que produzcan la imagen digitalizada de la firma, únicamente cuando los propios Usuarios realicen Operaciones Monetarias referidas al pago de bienes o servicios a través de dichas Terminales Punto de Venta.”.

firma-, 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.

Desde luego, tales pruebas o medios de convicción requerirán de la concurrencia de los correspondientes peritos o información de expertos.[50]

Aunado a que, como se precisó, los métodos de clonación de datos evolucionan de forma desmesurada, siendo que es responsabilidad de las instituciones financieras[51] 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, 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

[50] León Tovar, *Op. cit.* P. 72.
[51] "Artículo 107.- Serán responsabilidad del Destinatario y de la Parte que Confía, en su caso, las consecuencias jurídicas que entrañe el hecho de que no hayan tomado medidas razonables para:
I. Verificar la fiabilidad de la Firma Electrónica, o
II. Cuando la Firma Electrónica esté sustentada por un Certificado:
a) Verificar, incluso en forma inmediata, la validez, suspensión o revocación del Certificado, y
b) Tener en cuenta cualquier limitación de uso contenida en el Certificado.".

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, 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.

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 rubro y texto siguiente:

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”. Cuando se demanda 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, porque el usuario niega haberlos realizado, es la institución bancaria

quien está obligada a ofrecer las pruebas pertinentes que acrediten que fue el propio usuario quien realizó dicha transacción. Lo anterior encuentra justificación, porque con independencia de que la institución bancaria demandada exprese que la operación reclamada se efectuó a través de medios electrónicos utilizando la firma electrónica del cuentahabiente mediante el tecleo de su número de identificación personal (NIP), lo que presuntivamente acredita la existencia y validez de las transacciones; sin embargo, es ésta la que tiene la obligación de aportar las pruebas pertinentes con las que se demuestre que fue el propio usuario quien realizó tales operaciones, esto es, que se trató del emisor de la autorización mediante la firma electrónica. Ello, en virtud de 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 a efecto de poder verificar no sólo los montos de las disposiciones o los cargos, sino la efectiva utilización de la tarjeta que cuenta con mecanismo chip y del número de identificación personal de los usuarios. Por tanto, si la institución financiera quiere gozar de la presunción legal de tener como emisor al que envió el mensaje de datos, deberá 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; y 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. Sin que sea obstáculo a lo anterior, la regla establecida en el artículo 1196 del Código de Comercio de que corresponde probar al que niega, cuando al hacerlo desconoce la presunción legal que tiene a su favor el colitigante; pues si bien ello podría en principio trasladar la carga de la prueba al usuario, pues de conformidad con el artículo 90 Bis del mismo ordenamiento legal, la institución financiera cuenta con la presunción legal de tener como emisario al usuario y actuar en consecuencia cuando se haya aplicado el método de identificación

acordado, como puede ser el uso de la tarjeta bancaria al cual se encuentra integrado un chip con el número de identificación asociado, que una vez tecleado fue verificado por la institución bancaria dando como resultado que en el voucher se insertara la leyenda: *"NIP VERIFICADA o PIN VERIFIED"*; sin embargo para que el juez 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. Así, una vez que la institución bancaria haya acreditado que no se vulneró el sistema durante la transacción 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.

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 cuatro votos de los señores Ministros: Norma Lucía Piña Hernández, Jorge Mario Pardo Rebolledo (Ponente), Alfredo Gutiérrez Ortiz Mena y Presidente Juan Luis González Alcántara Carrancá. Ausente: Ministro Luis María Aguilar Morales.

Firman el Ministro Presidente de la Primera Sala y el Ministro Ponente con la Secretaria de Acuerdos que autoriza y da fe.

PRESIDENTE DE LA PRIMERA SALA:

MINISTRO JUAN LUIS GONZÁLEZ ALCÁNTARA CARRANCÁ.

PONENTE:

MINISTRO JORGE MARIO PARDO REBOLLEDO.

SECRETARIA DE ACUERDOS DE LA PRIMERA SALA:

LIC. MARÍA DE LOS ÁNGELES GUTIÉRREZ GATICA.

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.