AMPARO DIRECTO 20/2021
QUEJOSA PRINCIPAL: ***** ******** ** ******* ******** ******** ********** *** ***** ********** *******
QUEJOSA ADHESIVA: ***** ******* ******** ******* ** ******* ********
PONENTE: MAGISTRADO ALBERTO MIGUEL RUIZ MATÍAS
SECRETARIO: SHELIN JOSUÉ RODRÍGUEZ RAMÍREZ

Zapopan, Jalisco. Acuerdo del Segundo Tribunal Colegiado en Materia Civil del Tercer Circuito, correspondiente a la sesión virtual de **veintitrés de septiembre de dos mil veintiuno**.

V I S T O, para resolver el juicio de amparo directo **20/2021**; y,

R E S U L T A N D O S:

PRIMERO. Presentación de la demanda de amparo principal y adhesiva. En escrito presentado el **veintisiete de octubre de dos mil veinte**,[1] ***** ******** ** ******* ******** ******** ********** *** ***** ********** ******* (en lo sucesivo *"la quejosa"*, *"la peticionaria"* o *"la demandada"*), por conducto de su apoderada legal ***** *** ***** ******** *******, solicitó el amparo y protección de la Justicia Federal, contra el acto reclamado a la entonces **Juez Séptimo Especializado en Materia Oral Mercantil del Primer Partido Judicial del Estado de Jalisco**, actualmente denominada **Juez Décimo Séptimo en Materia Mercantil** de la misma circunscripción,[2] consistente en la sentencia definitiva de **ocho del mes y año precitados**, emitida en el juicio oral mercantil *******, así como al **secretario adscrito a tal órgano jurisdiccional**, a quien se le reclamó la ejecución de dicha determinación.

[1] Folios 9 a 63; *del expediente del juicio de amparo directo en el cual se actúa.*
[2] Según acuerdo SO.03.2020AGRAL del Consejo de la Judicatura del Estado de Jalisco.

Asimismo, en escrito presentado el **diecinueve de noviembre del año en mención**,[3] la tercera interesada ***** ******* ******** ******* ** ******* ******** (a quien en lo sucesivo se le denominará *"la tercera interesada"*, *"la adherente"* o *"la actora"*), presentó **amparo adhesivo**, en donde, entre otras cosas, hizo valer una causal de improcedencia del principal.

SEGUNDO. Trámite del amparo principal y adhesivo. De esa demanda constitucional principal correspondió conocer a este Tribunal Colegiado, cuyo Magistrado Presidente, en auto de **veinticuatro de febrero de dos mil veintiuno**,[4] la registró en el expediente **20/2021**; admitió tanto el amparo principal como el adhesivo; tuvo por rendido el informe justificado, reconoció el carácter de tercera interesada a ***** ******* ******** ******* ** ******* ********, y dio la intervención al respectiva al Agente del Ministerio Público de la Federación adscrito, quien no formuló alegato ministerial.

TERCERO. Emplazamiento de la tercera interesada. La constancia de emplazamiento de la tercera interesada en el principal no fue remitida por la autoridad responsable, sin embargo, en el auto admisorio citado en el resultando anterior se determinó que ello no era obstáculo para la integración de la relación jurídica en esta instancia constitucional, al ser evidente el conocimiento de la tercera interesada respecto de la demanda de amparo principal, pues promovió amparo adhesivo a la misma; de ahí que se calificara innecesario realizar el emplazamiento, conforme a

[3] Fojas 65 a 70; *ídem*.
[4] Folios 71 a 78; *ídem*.

la tesis de la Segunda Sala de la Suprema Corte de Justicia de la Nación, de rubro: ***"TERCERO PERJUDICADO QUE COMPARECE A JUICIO OPORTUNAMENTE SIN SER EMPLAZADO. NO ES NECESARIO PRACTICAR EL EMPLAZAMIENTO"***.[5]

CUARTO. Nueva integración y turno. En proveído de **veintiséis de marzo de dos mil veintiuno**,[6] se turnó el expediente al **Magistrado Alberto Miguel Ruiz Matías**, para la elaboración del proyecto de sentencia correspondiente, conforme al numeral 183 de la Ley de Amparo. Asimismo, en auto de **trece de agosto del año precitado**, se hizo constar que mediante oficio SEADS/454/2021, se comunicó la adscripción a este órgano jurisdiccional del **Magistrado Samuel Alberto Villanueva Orozco**, con efectos al dieciséis del mes y año mencionados en último término, por lo cual, se informó a las partes la nueva integración de este Tribunal a partir de la fecha indicada.

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

PRIMERO. Competencia. Este Segundo Tribunal Colegiado en Materia Civil del Tercer Circuito, tiene competencia legal para conocer y resolver el presente juicio de amparo, de conformidad con lo previsto en los numerales 37, fracción I, inciso c), 38, 144 y 145 de la Ley Orgánica del Poder Judicial de la Federación, y 186 de la Ley de Amparo, porque se reclama una sentencia definitiva emitida por una Juez Mercantil del Primer Partido Judicial del Estado de Jalisco, es decir, en la materia y adscripción en las cuales

[5] Localizable en Semanario Judicial de la Federación, Séptima Época, Volumen 217-228, Tercera Parte, página 117, registro 237141.
[6] Foja 88; *ídem*.

ejerce jurisdicción esta potestad constitucional. Asimismo, conforme a los Acuerdos Generales 8/2020, 10/2020, 12/2020 y 21/2020, éste último cuya vigencia fue ampliada por los diversos 25/2020, 37/2020, 1/2021, 5/2021 y 9/2021, todos del Pleno del Consejo de la Judicatura Federal, atinentes a las medidas de trabajo y contingencia, reanudación de plazos y regreso escalonado en los órganos jurisdiccionales, por el fenómeno de salud pública derivado del virus COVID-19.

SEGUNDO. Existencia del acto reclamado. La existencia del acto reclamado, consistente en la sentencia definitiva de **ocho de octubre de dos mil veinte**, quedó acreditada con las actuaciones originales remitidas por la autoridad responsable en apoyo a su informe justificado, en términos del numeral 178, fracción III, de la Ley de Amparo pues, tal resolución, obra glosada al expediente del juicio oral mercantil *******.

TERCERO. Legitimación. ***** ******** ** ******* ******** ******** ********** *** ***** ********** *******, como quejosa **principal**, está legitimada para promover la demanda constitucional, conforme al numeral 5, fracción I, de la Ley de Amparo;[7] ello, al ser parte demandada en el juicio natural.

[7] "Artículo 5o. Son partes en el juicio de amparo:
I. El quejoso, teniendo tal carácter quien aduce ser titular de un derecho subjetivo o de un interés legítimo individual o colectivo, siempre que alegue que la norma, acto u omisión reclamados violan los derechos previstos en el artículo 1o de la presente Ley y con ello se produzca una afectación real y actual a su esfera jurídica, ya sea de manera directa o en virtud de su especial situación frente al orden jurídico.
El interés simple, en ningún caso, podrá invocarse como interés legítimo. La autoridad pública no podrá invocar interés legítimo.
El juicio de amparo podrá promoverse conjuntamente por dos o más quejosos cuando resientan una afectación común en sus derechos o intereses, aun en el supuesto de que dicha afectación derive de actos distintos, si éstos les causan un perjuicio análogo y provienen de las mismas autoridades.

En tanto, ***** *** ***** ******** ******* tiene personería para promover la demanda de amparo **principal** en nombre de la persona jurídica en mención, pues la juez de origen la reconoció como apoderada legal de aquélla, mediante auto de **dieciocho de mayo de dos mil dieciocho**.[8]

Por su parte ***** ******* ******** ******* ** ******* ******** , como quejosa **adhesiva**, está legitimada para promover la demanda constitucional, conforme al numeral 182 de la Ley de Amparo, por ser tercera interesada en el principal, quien en parte obtuvo sentencia favorable, al decretarse la nulidad de la transferencia impugnada.

En tanto, ******* ******* ****** tiene personería para promover la demanda de amparo **adhesiva** en nombre de la persona jurídica mencionada en el párrafo anterior, pues la juez de origen lo reconoció como apoderado legal de aquélla, mediante auto de **veintinueve de marzo de dos mil dieciocho**.[9]

CUARTO. Oportunidad. La demanda constitucional principal se promovió oportunamente pues, la sentencia reclamada, se notificó a la quejosa ******** ** ******* ******** ******** ********** *** ***** ********** ******* por boletín judicial el **nueve de octubre de dos mil veinte**, por lo cual esa notificación surtió efectos el **trece**

Tratándose de actos o resoluciones provenientes de tribunales judiciales, administrativos, agrarios o del trabajo, el quejoso deberá aducir ser titular de un derecho subjetivo que se afecte de manera personal y directa;
La víctima u ofendido del delito podrán tener el carácter de quejosos en los términos de esta Ley".

[8] Fojas 68 y 69; *del expediente del juicio oral mercantil* *******.
[9] Foja 16; *ídem*.

siguiente, acorde con el precepto 1075 del Código de Comercio; en consecuencia, el plazo de quince días para promover la demanda, previsto en el artículo 17 de la Ley de Amparo, transcurrió del **catorce de octubre al cuatro de noviembre del año próximo pasado,** con excepción de los días **diez, once, diecisiete, dieciocho, veinticuatro, veinticinco y treinta y uno del primer mes citado, así como el uno del segundo en mención**, por haber sido inhábiles, con apoyo en el numeral 19 del ordenamiento mencionado en último término, igualmente el **doce de octubre y dos de noviembre del año precitado,** de conformidad con el numeral 55 del Código de Procedimientos Civiles del Estado de Jalisco, rector supletoriamente de la actividad de la autoridad responsable; en tanto, la demanda constitucional se presentó el **veintisiete de octubre de dos mil veinte**.

Tal cómputo puede constatarse en los siguientes calendarios:

OCTUBRE DE 2020						
Lunes	**Martes**	**Miércoles**	**Jueves**	**Viernes**	**Sábado**	**Domingo**
			1	2	3	4
5	6	7	8	**9** **Se notificó**	10	11
12 **Inhábil**	**13** **Surtió efectos**	**14 (1)** **Inició plazo**	**15 (2)**	**16(3)**	17	18
19 (4)	**20 (5)**	**21 (6)**	**22 (7)**	**23 (8)**	24	25
26 (9)	**27 (10)** **Presentó demanda de amparo**	**28 (11)**	**29 (12)**	**30 (13)**	31	

NOVIEMBRE DE 2020						
Lunes	**Martes**	**Miércoles**	**Jueves**	**Viernes**	**Sábado**	**Domingo**
						1
2 **Inhábil**	**3** **(14)**	4 **(15)** **Concluyó plazo**	5	6	7	8
9	10	11	12	13	14	15
16	17	18	**19** **Presentó demanda de amparo adhesivo**	20	21	22
23	24	25	26	27	28	29
30						

Por su parte, la demanda de amparo adhesivo se promovió oportunamente, pues el plazo de quince días previsto en el numeral 181 de la Ley de Amparo,[10] comenzó a transcurrir a partir del día siguiente de la notificación efectuada del auto admisorio del juicio principal, el cual se pronunció el veinticuatro de febrero de dos mil veintiuno; no obstante, en el caso, la demanda de amparo adhesivo se promovió con mucha anticipación, el diecinueve de noviembre de dos mil veinte,[11] de ahí que sea notoriamente oportuna y no se requiera realizar mayor cómputo.

QUINTO. Sentencia reclamada. Las consideraciones sustentadas en el fallo reclamado de **ocho**

[10] Artículo 181. Si el presidente del tribunal colegiado de circuito no encuentra motivo de improcedencia o defecto en el escrito de demanda, o si este último fuera subsanado, la admitirá y mandará notificar a las partes el acuerdo relativo, para que en el plazo de quince días presenten sus alegatos o promuevan amparo adhesivo.
[11] Fojas 65 a 70; *del cuaderno en que se actúa*.

de octubre de dos mil veinte se tienen a la vista al momento de resolver, porque está glosado al expediente del juicio oral mercantil ******* enviado por la autoridad responsable en apoyo a su informe justificado; por ende, es innecesaria su transcripción. Además, no existe precepto legal alguno en la Ley de Amparo que establezca tal obligación, y ese proceder no deja en estado de indefensión a las quejosas, porque con él no se viola ninguna formalidad del procedimiento.

En apoyo a lo anterior se cita, por analogía, la tesis aislada emitida por el entonces Segundo Tribunal Colegiado del Sexto Circuito,[12] de rubro y texto siguientes:

> ***"ACTO RECLAMADO. NO ES NECESARIO TRANSCRIBIR SU CONTENIDO EN LA SENTENCIA DE AMPARO.*** *De lo dispuesto por el artículo 77, fracción I, de la Ley de Amparo, sólo se infiere la exigencia relativa a que las sentencias que se dicten en los juicios de amparo contengan la fijación clara y precisa de los actos reclamados, y la apreciación de las pruebas conducentes para tener o no por demostrada su existencia legal, pero no la tocante a transcribir su contenido traducido en los fundamentos y motivos que los sustentan, sin que exista precepto alguno en la legislación invocada, que obligue al juzgador federal a llevar a cabo tal transcripción, y además, tal omisión en nada agravia al quejoso, si en la sentencia se realizó un examen de los fundamentos y motivos que sustentan los actos reclamados a la luz de los preceptos legales y constitucionales aplicables, y a la de los conceptos de violación esgrimidos por el peticionario de garantías."*.

SEXTO. Conceptos de violación. Las quejosas principal y adhesiva plantean como conceptos de violación,

[12] Localizable en la página 406, Tomo IX, abril de 1992, Octava Época, Semanario Judicial de la Federación y su Gaceta, registro 219558.

los expuestos en sus escritos por medio de los cuales promovieron la demanda de amparo correspondiente, respecto de los cuales tampoco existe obligación legal alguna de transcribirlos, pues, acorde con lo anterior, tales argumentos obran en autos.

Surge en apoyo a lo razonado, la jurisprudencia **2a./J. 58/2010**, sustentada por la Segunda Sala de la Suprema Corte de Justicia de la Nación,[13] cuyo texto es:

> "***CONCEPTOS DE VIOLACIÓN O AGRAVIOS. PARA CUMPLIR CON LOS PRINCIPIOS DE CONGRUENCIA Y EXHAUSTIVIDAD EN LAS SENTENCIAS DE AMPARO ES INNECESARIA SU TRANSCRIPCIÓN.*** *De los preceptos integrantes del capítulo X "De las sentencias", del título primero "Reglas generales", del libro primero "Del amparo en general", de la Ley de Amparo, no se advierte como obligación para el juzgador que transcriba los conceptos de violación o, en su caso, los agravios, para cumplir con los principios de congruencia y exhaustividad en las sentencias, pues tales principios se satisfacen cuando precisa los puntos sujetos a debate, derivados de la demanda de amparo o del escrito de expresión de agravios, los estudia y les da respuesta, la cual debe estar vinculada y corresponder a los planteamientos de legalidad o constitucionalidad efectivamente planteados en el pliego correspondiente, sin introducir aspectos distintos a los que conforman la litis. Sin embargo, no existe prohibición para hacer tal transcripción, quedando al prudente arbitrio del juzgador realizarla o no, atendiendo a las características especiales del caso, sin demérito de que para satisfacer los principios de exhaustividad y congruencia se estudien los planteamientos de legalidad o inconstitucionalidad que efectivamente se hayan hecho valer*.".

SÉPTIMO. Antecedentes destacados del asunto.

[13] Publicada en la página 830, Tomo XXXI, mayo de 2010, Novena Época, Semanario Judicial de la Federación y su Gaceta, registro 164618.

Para contextualizar el sentido de esta sentencia, a continuación se relatan algunos hechos obtenidos de las constancias del juicio de origen, las cuales, gozan de pleno valor probatorio, de conformidad con los preceptos 129,[14] 197,[15] y 202,[16] del Código Federal de Procedimientos Civiles, aplicados supletoriamente a la Ley de Amparo:

En escrito presentado el **veintitrés de marzo de dos mil dieciocho**,[17] ante la Oficialía de Partes del Consejo de la Judicatura del Estado de Jalisco, ***** ******* ******** ******** ** ******* ********, por conducto de su apoderado legal ******* ******* ****** presentó demanda en la vía ordinaria mercantil, contra la institución de crédito denominada ***** ******** ** ******** ******** ********** ********** *** ***** ********** ******* *** **********, ejerciendo la acción pago, fincada en la nulidad de cargos y operaciones bancarias no reconocidas, por lo cual reclamó las siguientes prestaciones:

> "(...) PRIMERA.- El pago, por concepto de reembolso, de la suma de ********** ******* ******** * ***** *** ********** ******* * ** ***** ** ********* **** de la que el banco demandado incurrió en responsabilidad al trasgredir, en perjuicio de la aquí parte actora, las disposiciones de Carácter General Aplicables a las Instituciones de Crédito, y cuyo derecho de pago se reclama, concretamente al incurrir la demandada, en

[14] **Artículo 129.-** Son documentos públicos aquellos cuya formación está encomendada por la ley, dentro de los límites de su competencia, a un funcionario público revestido de la fe pública, y los expedidos por funcionarios públicos, en el ejercicio de sus funciones.
[15] **Artículo 197.-** El tribunal goza de la más amplia libertad para hacer el análisis de las pruebas rendidas; para determinar el valor de las mismas, unas enfrente de las otras, y para fijar el resultado final de dicha valuación contradictoria; a no ser que la ley fije las reglas para hacer esta valuación, observando, sin embargo, respecto de cada especie de prueba, lo dispuesto en este capítulo.
[16] **Artículo 202.-** Los documentos públicos hacen prueba plena de los hechos legalmente afirmados por la autoridad de que aquéllos procedan; pero, si en ellos se contienen declaraciones de verdad o manifestaciones de hechos de particulares, los documentos sólo prueban plenamente que, ante la autoridad que los expidió, se hicieron tales declaraciones o manifestaciones; pero no prueban la verdad de lo declarado o manifestado.
[17] Fojas 1 a 15; ídem.

responsabilidad a su cargo, al fallar en su obligación de brindar seguridad a las operaciones de banca realizadas de manera electrónica, importe del que se dispuso por terceros, sin el consentimiento de esta accionante, en fecha 30 treinta de Mayo del año 2016 dos mil dieciséis mediante su disposición o cargo indebido, de la cuenta **** **** ***, con número de cliente ********.

SEGUNDA.- El pago de la indemnización que como intereses deba cubrir la Institución Financiera demandada a favor de la parte actora, sobre el capital de ********** ******* ******** * ***** *** ********** ******* * ** ***** ********** ***** desde el día 30 de mayo del año 2016 dos mil dieciséis y hasta el día en que cumpla con su obligación de pago, siendo esa suma la dispuesta y esa fecha, en que de manera ilegal y sin consentimiento del titular de la cuenta **** **** ***, se dispuso de manera electrónica en su perjuicio, al fallar los sistemas de seguridad electrónica del (sic) la Institución Financiera demandada ******** o con complicidad de su personal, y cuyo reembolso le fue solicitado desde el día inmediato siguiente al que se efectuó de manera ilegítima, el cargo a la cuenta de esta actora, habiéndose negado expresamente la Institución Financiera ******* ahora demandada, a restituirla a su cliente. Por equidad esta indemnización la solicito sobre el mismo parámetro de la tasa anual moratoria que cobra el banco a su favor cuando sus clientes incurren en mora respecto de créditos contratados y el banco se erige en acreedor. El importe líquido de esta prestación se determinará en ejecución de sentencia sin dejar de asentar que el pago de intereses nunca podrá ser inferior al interés legal.

TERCERA.- Por el pago de los daños y perjuicios con los que la aquí actora se ha visto y se siga viendo afectada, como consecuencia de la necesidad de tener que recurrir a la continuación de servicios profesionales y realizar gastos, para tener que reclamar de *******, primero ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, y después demandarles judicialmente, la restitución del dinero de mi representada que reclama como primera prestación; esto es, se ha tenido que contratar los servicios de un abogado, lo que implica, se ha tenido que erogar en el pago de servicios de un notario público, durante el juicio podrían generarse los

pagos de copias y honorarios de peritos, todo lo cual, si bien podría ser incluido en el conceptos de gastos y costas, se reclama como un derecho por concepto de daños y perjuicios, porque implica una afectación económica en mi poderdante, al verse obligada a realizar erogaciones de dinero, distrayendo ese recurso, de los fines distintos a los del objeto social de mi poderdante, todo como consecuencia de la negativa del banco demandado de restituir el dinero cuando le fue reclamado de manera directa, de ahí que se solicite que se condene a la demandada, al pago de este concepto de daños y perjuicios porque a causa de la negativa infundada del enjuiciado, se ocasiona una pérdida, un menoscabo o privación en afectación de la aquí parte actora, erogaciones que dado que se gestan durante el curso del juicio, no podrán ser cuantificados y liquidados, sino hasta una vez que finalice este juicio, de ahí que pido se decrete su procedencia y reservase su determinación hasta el procedimiento de ejecución de sentencia.
CUARTA.- Por el pago de los gastos y costas que la conducta de mala fe del banco demandado, han ocasionado al punto que tener que llegar a promover este juicio".

En auto de **seis de abril de dos mil dieciocho**,[18] previo desahogo de la prevención formulada al actor para corregir la vía por media de la cual pretendía encausar su solicitud, la **Juez Séptimo Especializado en Materia Oral Mercantil del Primer Partido Judicial del Estado de JAlisco**, en lo interesante, radicó la demanda en el expediente *******, la admitió en la vía oral mercantil, y ordenó emplazar a la institución bancaria demandada.

Mediante escrito presentado el **catorce de mayo de dos mil dieciocho**,[19] ***** ******** ** ******** ********* ********** ********** *** ***** ********** *******, por

[18] Fojas 20 y 21; *ídem*.
[19] Fojas 26 a 67; *ídem.*

conducto de su apoderada general para pleitos y cobranzas, dio contestación a la demanda promovida en su contra.

En proveído de **dieciocho de mayo de dos mil dieciocho**,[20] la juez de instancia tuvo por contestada oportunamente la demanda y por ofrecidas las pruebas respectivas, con lo cual ordenó dar vista a la actora.

Mediante escrito presentado el **veinticuatro de mayo de dos mil dieciocho**,[21] la actora desahogó la vista correspondiente.

En proveído de **treinta de mayo de dos mil dieciocho**,[22] entre otros aspectos, la juez de origen tuvo por desahogada la vista con la contestación de la demanda, así como señaló hora y fecha para el desahogo de la audiencia preliminar. En acta de **catorce de junio del año precitado**,[23] se hizo constar la celebración de tal audiencia.

El **catorce de agosto de dos mil dieciocho**,[24] se desahogó la audiencia de juicio y, en lo interesante, ante la notoria contradicción en las conclusiones de los dictámenes emitidos por los peritos designados por las partes, la juez responsable consideró necesario designar un **perito tercero para el caso de discordia**.

[20] Fojas 68 y 69; *ídem*.
[21] Fojas 70 y 71; *ídem*.
[22] Fojas 72 y 73; *ídem*.
[23] Fojas 80 a 83; *ídem*.
[24] Fojas 117 a 119; *ídem*.

El **cuatro de julio de dos mil diecinueve**,[25] se reanudó la audiencia de juicio, para el desahogo de diversas probanzas ofertadas por las partes; luego, el **ocho de agosto del mismo año al reanudarse la audiencia de juicio**[26] y se fijó fecha para el dictado de la sentencia correspondiente, la cual se emitió el **quince de agosto de dicho año**,[27] en la cual se determinó que la actora probó los hechos constitutivos de la acción ejercitada, y la demandada justificó parcialmente sus excepciones, por lo cual, en lo interesante, se declaró la nulidad absoluta respecto de la transferencia efectuada en la cuenta número **** **** *** el treinta de mayo de dos mil dieciséis, por el importe de ********** ******* ******** * ***** *** ********** ******* * ** ***** ****** ****** *********; en consecuencia, se condenó a la parte demandada a pagar a la actora la cantidad mencionada con antelación por concepto de suerte principal, resultado de la transferencia no reconocida.

Esa sentencia de **quince de agosto de dos mil diecinueve** fue señalada como acto reclamado por la hoy quejosa en la demanda de amparo directo generadora del expediente ******** cuyo conocimiento correspondió a este Tribunal, el que en sentencia de **veintitrés de junio de dos mil veinte**,[28] concedió la protección constitucional para los efectos siguientes:

> "1) Que la responsable deje insubsistente la sentencia reclamada de quince de agosto de dos mil diecinueve.
>
> 2) Hecho lo anterior, dicte una nueva sentencia en la

[25] Fojas 165 y 166; *ídem*.
[26] Fojas 172 a 176; *ídem*.
[27] Fojas 179 a 223; *ídem*.
[28] Fojas 279 a 308; *ídem*.

cual, conforme los lineamientos de esta ejecutoria y acorde a los principios de congruencia y exhaustividad, analice los dictámenes periciales rendidos, sobre la base de que en ellos se realizaron señalamientos en relación a las medidas de seguridad que mencionaron los expertos que tenía el portal de internet de la institución crediticia demandada en la fecha en la cual se realizó la transacción materia de litigio, las cuales guardan relación con las acciones y defensas hechas valer en el juicio, a fin de que determine lo que proceda sobre el alcance de dichas pruebas para demostrar la fiabilidad y seguridad o no de la plataforma donde se realizó la operación bancaria.

3) Resuelva lo que legalmente proceda con plenitud de jurisdicción".

En cumplimiento a ese fallo protector, el juez mercantil emitió sentencia el **ocho de octubre de dos mil veinte**,[29] en la cual, en lo interesante, nuevamente decretó la nulidad de la transferencia impugnada realizada a través de la cuenta **** **** ***, y condenó a la enjuciada al pago de la suerte principal de ********** ******* ******** * ***** *** ********** ******* * ** ***** ****** ****** *********, resultante de la transferencia no reconocida ni autorizada por la actora.

Esa sentencia, acorde con lo establecido por el numeral 170 de la Ley de Amparo, **constituye el acto reclamado en el presente juicio constitucional**.

OCTAVO. Se desestima causal de improcedencia. Antes de responder los conceptos de violación formulados en la demanda de amparo **principal**, es necesario analizar las causales de improcedencia hechas valer en su contra, por ser una cuestión de orden público y de estudio preferente, ya sea

[29] Fojas 310 a 364; *ídem*.

que lo hagan valer las partes o que el órgano jurisdiccional lo advierta de oficio, de acuerdo con lo previsto en el artículo 62 de la Ley de Amparo.

Al respecto, la tercera interesada en el principal y quejosa adhesiva, en una parte de su escrito de demanda de amparo adhesivo, aduce que, a su criterio, en la especie se actualiza la causal de improcedencia prevista en el numeral 61, fracción XXII, de la Ley de Amparo,[30] básicamente, porque *"si bien es cierto subsiste el acto reclamado no menos cierto resulta, que el mismo no surte efecto alguno, lo anterior, en razón de que esta parte quejosa, acredité todos y cada uno de mis acciones* (sic) *en el juicio de origen, tal y como se desprende de actuaciones, por lo que el presente juicio resulta por demás inoperante. Por lo que solicito se actualice las causales de improcedencia mencionadas y por lo tanto sobreseimiento este juzgado federal las exime de oficio y las declare de pleno derecho"*.

Tales argumentos son **infundados**, porque la quejosa adherente hace depender la aplicabilidad de la causal en aspectos de fondo de la litis de origen, y no de estricta procedencia del amparo directo; ello, al afirmar que por haber demostrado cada una de sus "acciones" en el juicio oral mercantil, debe declararse improcedente el presente asunto, aspecto en el cual es inviable sustentar dicho motivo de inejercitabilidad, pues para dilucidar si la adherente efectivamente acreditó o no su acción natural, tendrían que abordarse aspectos de fondo relacionados con la materia de

[30] "Artículo 61. El juicio de amparo es improcedente:
XXII. Cuando subsista el acto reclamado pero no pueda surtir efecto legal o material alguno por haber dejado de existir el objeto o la materia del mismo".

los conceptos de violación principales pues, precisamente, los argumentos del banco en el principal inciden en si se demostraron o no los elementos de la acción ejercida; de ahí lo inexacto de los planteamientos de la adherente, por pretender sustentar la improcedencia del juicio de amparo directo en aspectos de fondo.

Ello, sobre la base de que las causales de improcedencia del juicio de amparo deben ser claras e inobjetables, de lo cual se desprende que si se hace valer una en la cual, como en el caso, se involucra una argumentación íntimamente relacionada con el fondo del negocio, debe desestimarse.

Tiene aplicación al caso, la jurisprudencia **135/2001**,[31] sustentada por el Pleno de la Suprema Corte de Justicia de la Nación, del contenido siguiente:

> ***"IMPROCEDENCIA DEL JUICIO DE AMPARO. SI SE HACE VALER UNA CAUSAL QUE INVOLUCRA EL ESTUDIO DE FONDO DEL ASUNTO, DEBERÁ DESESTIMARSE.*** *Las causales de improcedencia del juicio de garantías deben ser claras e inobjetables, de lo que se desprende que si se hace valer una en la que se involucre una argumentación íntimamente relacionada con el fondo del negocio, debe desestimarse".*

Con independencia de lo expuesto, la causal de improcedencia citada por la adherente es **inaplicable**, porque la hipótesis normativa establecida en el numeral 61, fracción XXII, de la Ley de Amparo, se circunscribe a: "*cuando subsista el acto reclamado pero no pueda surtir efecto legal o*

[31] Publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XV, enero de 2002, página 5, registro 187973.

material alguno por haber dejado de existir el objeto o la materia del mismo", lo cual en la especie no opera, pues el acto reclamado es una sentencia mercantil cuya ejecución o materialización, en principio, sólo depende del resultado del presente juicio de amparo directo principal; de ahí que sí pueda surtir efectos legales o materiales, y sí exista el objeto o la materia del mismo.

Superado lo previo y al no haberse formulado alguna otra causal de improcedencia por las partes, ni advertir este Tribunal alguna otra que sea de obvia y objetiva constatación, procede analizar los conceptos de violación planteados en la demanda de amparo directo principal.

NOVENO. Estudio del amparo principal. Los conceptos de violación principales son ***infundados*** en una parte e ***inoperantes*** en otra, los cuales, a fin de resolver la cuestión efectivamente planteada, serán analizados en un orden diverso al propuesto, con fundamento en el artículo 76 de la Ley de Amparo.

Para justificar tal calificativa, primeramente debe destacarse que en su demanda mercantil inicial la actora circunscribió la litis a la nulidad de la transferencia por banca electrónica realizada de su cuenta **** **** *** por la cantidad de ********** ******* ******** * ***** *** ********** ******* * ** ***** ********** ****, a las 14:43 horas del treinta de mayo de dos mil dieciséis, en favor de un supuesto tercero, con cuenta terminación 048 de nombre "***** ** **** *".

Además, la actora, por conducto de su apoderado legal ******* ******* ****** negó haber otorgado su **consentimiento o autorizado** el alta y transferencia de los recursos mencionados y, en lo interesante, manifestó que a la hora en la cual se realizó el movimiento él y ***** ********* ******** *******, ambos socios de la accionante (****** ******* ******** ******* ** ******* ********), se encontraban en *"horas de comida"*, por lo cual cada quien tenían sus dispositivos de banca electrónica *"Netkey"*, por lo cual tan pronto se percataron del alta y la transferencia procedieron a *"bloquear el usuario desconocido, y retirar dinero restante de esa cuenta, ya que teníamos el temor fundado de que el robo se hiciera más extenso* (sic)*"*.

La accionante manifestó que el dispositivo Netkey sirve para utilizarse en operaciones de banca electrónica a través de internet, consistiendo en un reloj interno, el cual sincroniza con un servidor de cómputo del banco a la hora de ser activado por primera vez, y tiene como finalidad establecer una contraseña única en un periodo de tiempo, no más de un minuto, mostrando una pantalla, con un algoritmo secreto y privado, que permite el uso de los servicios bancarios.

Igualmente, la actora narró que reportaron el robo ante la institución bancaria *******, a lo cual les otorgaron un número de reclamación, en el cual dicho banco emitió una carta de rechazo, bajo el argumento de que la operación se realizó con sus firmas digitales, sin mencionar, entre otras cosas, **"desde que IP fue realizado"**.

Además, la accionante manifestó el ser *"de todos conocido que, cuando se realiza un movimiento a través de* ***** ***, *se genera una dirección IP, que es la manera en que los equipos comunican a través de internet mediante el protocolo IP (protocolo de internet). Este protocolo utiliza direcciones numéricas denominadas direcciones IP. Los equipos de una red utilizan estas direcciones para comunicarse de manera que cada equipo de la red tiene una dirección exclusiva. Por lo que en un razonamiento sistemático, si la operación no reconocida por mi poderdante hubiera sido consentida, tal y como lo afirma la institución, sería evidente que el cargo realizado a las 14:43 hrs el día 30 de mayo del 2016 dos mil dieciséis, tendría la misma dirección IP que la operación donde mi representada extrajo el dinero restante cuando se dio cuenta del robo, siendo lo anterior imposible, ya que como se ha venido mencionando, el suscrito a la hora de la extracción, contaba con los dispositivos móviles en su poder. Lo anterior permite revelar que los sistemas de seguridad informática de* *******, *fallaron ya que debió crear un bloqueo de seguridad, lo cual se evidencia en la divergencia de la dirección IP, entre la objetada y la realizada por el suscrito*".

Ahora, al contestar la demanda, en lo interesante, afirmó que la transferencia cuya nulidad se demandó es válida, esencialmente, porque los datos de **autenticación** del usuario fueron expresados correctamente para la autorización de la transacción, de quien dijo utilizó su *"firma electrónica"* y *"netkey"* y, en relación con la dirección IP desde la cual manifestó que se llevó a cabo la operación, fue la de número "**31.168.172.139**", aunque a su criterio es *"irrelevante el lugar*

físico en donde se encontraren y/o las actividades que conjunta o separadamente realizaban las personas antes mencionadas", porque con *"**los medios de autenticación es posible se transmitan por algún sistema de voz o de datos que permitan en tiempo real que cualquier tercero conozca la firma electrónica y las claves dinámicas, no sólo en México, sino en cualquier parte del mundo"***.

Cabe mencionar que en tal contestación de demanda la enjuiciada, aquí quejosa, transcribió una parte de la *"solicitud única* ******* *"* relativa al contrato de banca electrónica celebrado entre las partes, con *"**domicilio principal"*** en la colonia ******** ********** , Guadalajara, Jalisco, México.

Ahora, en la sentencia reclamada de **ocho de octubre de dos mil veinte**, en lo interesante, concluyó que el banco no demostró que la operación bancaria impugnada haya sido fiable y segura como para considerar que la actora expresó su verdadero consentimiento (más allá de haberse utilizado sus claves), particularmente, porque quedó demostrado que el IP desde donde se autorizó la transacción corresponde a la ubicación geográfica del país de Israel, lo cual era algo **inusual** y, por seguridad, debió de optar por las medidas necesarias para evitar *"el robo de identidad"*; tal como se advierte de la siguiente transcripción:

> "[...] Lo anterior, se puede acreditar, a guisa de ejemplo, ofreciendo la opinión de un experto en la materia informática que dirima si la plataforma donde se realizó una operación bancaria es fiable y segura por contar con un procedimiento que invariablemente autorizará una transacción siempre que se ingresen los datos correctos requeridos (usuarios, claves, NIP,

contraseñas dinámicas, etcétera), sin embargo, en el caso a estudio aun cuando la demandada ofertó una prueba pericial en dicha materia, la misma quedó superada con el dictamen pericial emitido por el experto designado como tercero en discordia, quien precisó que ningún sistema computacional es seguro al cien por ciento, por lo que es altamente recomendable que las instituciones bancarias revisen constantemente sus medidas de seguridad, tan es así que en dicha página alertan sobre fraudes que han ocurrido y que dicha página no cuenta con la opción que permitiera instalar la herramienta anti-intrusos, que si bien contaba con la utilización del protocolo HTTPS que encripta la información que se intercambia entre banco y usuario y es más difícill que pueda ser visualizada por algún intruso, sin embargo, se han encontrado con ciertas vulnerabilidades que un atacante puede aprobechar para obtener información sensible, por lo cual no se puede determinar que el portal de banca electrónica sea totalmente seguro y fiable; razón por la cual se concluye que no existe la certeza de que la parte actora hubiese realizado u otorgado su consentimiento para que se llevara controversia, toda vez que la IP con la que se realizó la transferencia materia del juicio no era la usual que utilizaba la parte actora; por lo tanto, la institución bancaria demandada, debió de optar las medidas necesarias para evitar el robo de identidad.

De tal modo que para que operen a favor de una institución bancaria las presunciones previstas en los citados artículos 90 y 95 del Código de Comercio, esto es, para presumir que una transacción realizada se ejecutó por el emisor (cuentahabiente), al ser éste el único que cuenta con la información requerida para tal efecto (claves, NIP, contraseñas dinámicas, etcétera), previamente, el banco debe acreditar que la plataforma donde se ejecutó la operación es fiable y segura y que existe la certeza de que una transacción sólo se realizará si se ingresan los datos correctos y, de ese modo, se revertirá la carga de la prueba al usuario bancario para que acredite que los mensajes de datos de la operación que controvierte no fueron emitidos por él o por alguien a quien autorizó o por un sistema de información que programó para actuar en su nombre automáticamente.

[...] Por tanto, contrario a lo alegado por la parte demandada y en respuesta al planteamiento que se

analiza, se arriba a la conclusión de que evidentemente bajo todos los razonamientos incoados en el cuerpo normativo de esta resolución le corresponde a la institución de crédito demandada, la carga de justificar que el actor hizo uso de su dispositivo identificado como "Netkey", y que en todo caso la plataforma del banco cumple con los requisitos establecidos para la verificación de la fiabilidad de las firmas electrónicas (fiabilidad de la plataforma para verificar la firma electrónica) de tal forma que exista certeza de que los mensajes de datos ingresados que motiven una operación efectivamente provienen del emisor (cuentahabiente), ello a fin de evitar intrusiones por delincuentes cibernéticos o fraudes de esa naturaleza [...].

Se sostiene lo anterior, al haber quedado demostrado que la IP desde la cual se inició la sesión y que también de la que se originó la transacción en litis, muestra que este rango pertenece a un área geográfica de Israel, por lo que quien lo realizó si bien pudo estar realmente ubicada en Israel o en otra ubicación incluyendo México, al haber cambiado su IP mediante algún programa de los gratuitos de la red con el fin de evitar su rastreo, al haber detectado la institución bancaria demandada que la IP con la que se realizó la transferencia materia de este juicio no era la usual que utilizaba la parte actora, debió de optar las medidas necesarias para evitar el robo de identidad; por lo tanto, en el caso concreto no se tomaron medidas de seguridad adecuadas para la autenticación y seguridad del usuario bancario.

En consecuencia, se declara la nulidad absoluta respecto de la transferencia efectuada de la cuenta número **** **** *** siendo esta la efectuada el día 30 treinta de mayo del año 2016 dos mil dieciséis, por el importe ** ********** ******* ******** * ***** *** ********** *** **** * ** ***** ****** ****** *********".

Sentado lo anterior, primeramente debe indicarse que son ***infundados*** los conceptos de violación en los cuales la quejosa argumenta que *"el perito no pudo asegurar con certeza la ubicación de la IP"*, pues basta imponerse del

dictamen emitido por el diestro tercero en discordia para advertir que determinó con precisión que la IP con número "**31.168.172.139**", desde la cual se inició la sesión y se originó la transacción impugnada, pertenece al área geográfica de Israel, y que esto sólo podía significar dos cosas:

1) Que quien realizó la transacción, al hacer uso de las claves confidenciales de la actora, verdaderamente se encontraba en Israel; o,

2) Que, desde un lugar distinto, utilizó un programa para disfrazar la IP a fin de evitar ser rastreado.

Para mejor referencia, a continuación se realiza la transcripción correspondiente:

> "5.5. Que la IP 31.168.172.139 desde la cual se inició la sesión y que también de la que se originó la transacción en litis, muestra que este rango pertenece a un área geográfica de Israel, como lo indico con la figura sacada de la página: https://www.ip-adress.com/ipv4/31.168.172.139, que se utiliza para geolocalizar IP'S *[inserta imagen].*
> 5.11. Para terminar, quien realizó la transacción en litis, la pudo realizar con esa IP "rara" 31.168.172.139 porque estaba realmente ubicado en Israel o porque estando en otra ubicación geográfica, incluyendo México, haya cambiado este IP mediante algún programa de los que existen hasta gratuitos en internet, el cual permite seleccionar una IP de cualquier parte del mundo, con el fin de evitar su rastreo, y que conocía además los factores de autenticación del operador 4, es decir de la parte actora, siguiendo con la transferencia electrónica, esta fue realizada a la cuenta ******* *******, y que según el ejecutivo de cuenta entrevistado, esta cuenta pertenece la *(sic)* zona de ******* ********* ******.

En relación con la posibilidad de llegar a conocer los factores de autenticación se pueden utilizar una técnica o combinación de técnicas de ingeniería social como pishing (correos falsos), vishing (llamadas telefónicas falsas), pharming (páginas web falsas), smishing (mensajes de texto falsos), entre otras, realizando con ellas el robo de identidad.
Dadas las actuales tendencias crecientes de los ataques cibernéticos en especial en las instituciones bancarias, es altamente recomendable que ellas tomen mayores medidas de seguridad, como por ejemplo utilizar los factores de autenticación de categoría 4: técnicas biométricas) para que al realizar una transacción el usuario sea quien dice ser y no se pueda permitir que esta información caiga en manos de un tercero.
Aunado a esto se necesita una mejor capacitación del eslabón más débil de la cadena que es el usuario (el cuenta habiente en este caso).
Finalmente se ocupa una mayor cultura de prevención (alertar), tanto de las empresas como en el personal ya que las alarmas suceden cuando la vulnerabilidad ha sido afectada".

Así, **contrario a lo afirmado por la quejosa**, el diestro fue categórico al indicar que con la IP "**31.168.172.139**" se originó la transacción impugnada y que ésta corresponde a la ubicación del país de Israel, ya sea porque la persona que realizó la operación verdaderamente se encontraba en ese lugar o utilizó esa dirección a través de un programa para evitar su rastreo, y que si bien aquélla conocía los factores de autenticación del operador 4, es decir, de la actora, pudo obtenerlos a través de correos, llamadas telefónicas, páginas web o mensajes de textos falsos, entre otras técnicas de ingeniería social para el robo de identidad.

De este modo, ante lo ***infundado*** del indicado concepto de violación, queda firme la consideración toral de la

sentencia reclamada relativa a que la **IP 31.168.172.139** corresponde al territorio de Israel; lo anterior, en la inteligencia de que esa IP fue reconocida por la propia peticionaria desde la contestación de la demanda como aquélla de donde se realizó la operación impugnada, en los términos literales siguientes:

> "Señalando desde este preciso instante que la dirección IP desde la cual se llevó a cabo la operación **31.168.172.139**".

En otro orden, la quejosa argumenta esencialmente que es intrascendente el lugar al cual corresponde la IP de donde se realizó la transacción, porque las operaciones pueden realizarse desde cualquier parte siempre y cuando se cuenten con las claves correctas, mismas que pueden transmitirse de manera remota.

La peticionaria agrega que incluso de la videograbación de la audiencia especial donde la demandada cuestionó al perito tercero en discordia reconoció tal intrascendencia, pues al preguntarle en vía de ejemplo que si por teléfono se le podrían proporcionar las claves a un tercero en otra parte y éste las operaba en ese momento, se podrían realizar las transferencias, a lo cual el perito contestó que sí y con ello aceptó que la IP resultaba intrascendente, por ser posible lo anterior; asimismo, que no es relevante desde cuál IP se realizaron las transacciones, porque precisamente la ventaja de la banca electrónica es que se pueda operar desde diversas partes del mundo incluso desde *"Rusia, Afganistán, Israel, Estados Unidos, etc. sin que ello implique por sí mismo que las mismas son fraudulentas. Por el contrario, sin*

importar el lugar o país, se requiere como los mismos peritos aceptaron en sus dictámenes la presencia de los siete facturas de seguridad, los cuales estuvieron presentes, ya que de otra forma no se hubiese logrado concretar la transferencia".

Tales conceptos de violación son ***infundados*** pues, en oposición a lo afirmado repetitivamente por la inconforme, el hecho de que el protocolo o dirección de internet (IP) desde la cual se originó la transacción impugnada pertenezca al área geográfica de Israel **sí es trascendente para calificar como objetivamente correcta la decisión de la juez responsable en cuanto a la falta de fiabilidad del sistema electrónico bancario, pues se trata de una operación inusual que evidencia tal deficiencia la cual impide aceptar la presunción de que, al haberse utilizado en la transacción las credenciales o claves de autenticación de la actora, efectivamente fue ésta quien realizó o autorizó la operación**.

Ese tema fue resuelto por la Primera Sala de la Suprema Corte de Justicia de la Nación, en la ejecutoria de la contradicción de tesis 206/2020, resuelta el **diecisiete de marzo de dos mil veintiuno**, lo cual no puede ser discutido de ninguna manera por este Tribunal en términos del numeral 217 de la Ley de Amparo y ahí, en lo interesante, la superioridad determinó lo siguiente:

> **"[...] c) Seguridad de la banca electrónica.**
> Sobre este aspecto, debe señalarse que, al igual que la vulnerabilidad que representan las transacciones utilizando una tarjeta con mecanismo chip y número de identificación,

como fue estudiado en la Contradicción de Tesis 128/2018; la revolución digital que está transformando la banca por internet también enfrenta desafíos cibernéticos en su funcionamiento.

Existen diversos riesgos asociados a la banca electrónica, ya sean estratégicos, operativos, legales y reputacionales. El riesgo operativo se encuentra estrechamente vinculado con los mecanismos de seguridad que pueden implementarse para evitar vulneraciones a los sistemas establecidos para el correcto desarrollo transaccional; no obstante, con este tipo de riesgo también pudiera verse ligada a la institución en afectaciones legales y reputacionales[32]. Por ejemplo, cuando se detecta una violación a la seguridad de la plataforma donde se permitiera acceso no autorizado a la información de clientes, no solo expone al banco a verificar la transferencia no reconocida, sino que también puede generar conflictos legales y riesgo en la reputación de la institución por el manejo defectuoso de sus sistemas.

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

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

Este tipo de sistemas, como todo avance tecnológico, ha demostrado diferentes cualidades para constituirse como una tecnología que vuelve más eficiente la prestación de servicios, pero que no se encuentra libre de riesgos de seguridad en su operación[33]. Por ende, como cualquier servicio que dependa de una infraestructura tecnológica, es susceptible de intromisiones directas o indirectas que vician su operación, es necesario analizar el grado del ataque en cuanto a intensidad, habilidad y persistencia.[34]

Incluso, el gran volumen de transacciones digitales significa que los métodos manuales tradicionales de monitoreo y detección de fraude no tienen la capacidad ni la velocidad

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

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

[34] Ullah Khan, Hammed. Op. cit.

para enfrentar el desafío al que se enfrentan los bancos en la actualidad[35].

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

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

- Virus: Sección oculta y auto replicante de software informático, que se propaga al infectar (es decir, al insertar una copia de sí mismo en otro programa y convertirse en parte de él). Un virus no puede correr solo; requiere que su programa huésped se ejecute para activarlo.
- Spyware: Software que se instala de forma secreta o subrepticia en un sistema de información para recopilar información sobre individuos u organizaciones sin su conocimiento.
- Adware: Software que reproduce, muestra o descarga automáticamente material publicitario a una computadora después de instalar el software o mientras se utiliza la aplicación. El programa malicioso está diseñado para mostrar publicidades no deseadas en la computadora de la víctima sin su permiso, los pop-ups o anuncios son incontrolables y tienden a comportarse de forma errática, por lo general aparecen muchas veces en la pantalla y resulta tedioso cerrarlos.
- Rootkit: Un conjunto de herramientas utilizadas por un atacante después de obtener acceso al nivel de raíz en un host para ocultar las actividades del atacante en el host y permitirle mantener el acceso de nivel de raíz “root” al host a través de medios secretos. En otras palabras, permite a un pirata informático acceder o controlar de forma remota un dispositivo informático o una red sin estar expuesto. Son difíciles de detectar debido a que se activan incluso antes de que se inicie el sistema operativo del sistema.
- Trojan Horse: Programa de computadora que parece tener una función útil, pero también tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces explotando autorizaciones legítimas de una entidad que invoca el programa.
- Worm: Es el término simplificado para denotar “write once, read many”, consiste en un programa informático que puede ejecutarse de forma independiente, puede propagar una

[35] Net Guardians. “Digital banking fraud: Best practice for technology-based prevention”. Recuperado de: “*https://netguardians.ch/digital-banking-fraud/*”

versión completa de sí mismo en otros host o redes y puede consumir los recursos de una computadora de manera destructiva. En otras palabras, es un código malicioso que se copia asimismo y se esparce hacia otras computadoras, un sistema o red.

- Ransomware: Es un virus que impide que el usuario acceda a los archivos o programas y para su eliminación se exige pagar un “rescate” a través de ciertos métodos de pago en línea. Una vez pagada la cantidad, el usuario puede reanudar el uso de su sistema.
- Keylogger: Un programa diseñado para registrar qué teclas se presionan en un teclado de computadora que se usa, para obtener contraseñas o claves de cifrado.
- Botnet: Es una red de dispositivos que se ha infectado con software malintencionado, como un virus. Los atacantes pueden controlar una botnet como grupo sin el conocimiento del propietario con el objetivo de aumentar la magnitud de sus ataques. A menudo, una botnet se usa para abrumar a los sistemas en un ataque de denegación de servicio distribuido (DDoS).

B. **Phishing.** Una técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta en un correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por un negocio legítimo o una persona con reputación.

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

D. **Distributed denial-of-service attack (DDoS).** Un ataque de denegación de servicio inunda sistemas, servidores o redes con tráfico para agotar los recursos y el ancho de banda. Como resultado, el sistema no puede cumplir con solicitudes legítimas. A veces el atacante puede inyectar y ejecutar un código arbitrario mientras realiza un ataque DoS para acceder a la información o ejecutar comandos en el servidor. Este tipo de ataque degrada significativamente el servicio y la calidad experimentada por usuarios legítimos, pues introduce grandes retrasos en la respuesta del sistema[36]. Los atacantes también pueden usar múltiples dispositivos comprometidos para lanzar este ataque. Esto se conoce como un ataque de denegación de servicio distribuido.

[36] Ullah Khan, Hammed. Op. cit.

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

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

Por su parte, en relación con la calidad operacional de banca por internet, The Open Web Application Security Project (OWASP)[37] ha clasificado los riesgos de seguridad en las aplicaciones de red de acuerdo con los ataques exitosos ocurridos.

Entre los ataques informados[38], encontramos los siguientes:

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

II) **Cross-Site Scripting (XSS)**. Se suscitan cada vez que una aplicación toma datos no confiables y envía a un navegador web sin la validación adecuada, para luego escapar. Este tipo de mecanismo permite a los atacantes ejecutar *scripts* en el navegador de la víctima que incluso puede llegar a secuestrar sesiones de usuario, desfigurar sitios web o redirigir al usuario a sitios maliciosos.

[37] Open Web Application Security Project® (OWASP) es una fundación sin fines de lucro que trabaja para mejorar la seguridad de los softwares, a través de proyectos de código abierto liderados por diversos miembros expertos en desarrollo tecnológico para proteger la web. "https://owasp.org/#"
[38] Ullah Khan, Hammed. Op. cit.

III) **Broken Authentication and Session Management (BA&SM)**. Este tipo de funciones posibilitan a los atacantes comprometer contraseñas, claves, tokens de sesión, o explotar otras fallas de implementación para asumir las identidades de otros usuarios. El objetivo de este ataque es apoderarse de una o más cuentas obteniendo los mismos privilegios que el usuario real.

IV) **Insecure Direct Object References (IDOR).** La referencia de objeto ocurre cuando un desarrollador expone una referencia a un objeto de implementación interno, como, un archivo, un directorio o una clave de base de datos. Sin un acceso de control u otra protección, los atacantes pueden manipular estas referencias para acceder a datos no autorizados de otras personas.

V) **Cross-Site Request Forgery (CSRF).** Este tipo de ataque obliga a iniciar sesión en el navegador de la víctima para enviar una solicitud HTTP falsificada, incluida la *cookie*[39] de sesión de la víctima y cualquier otra información de autenticación incluida automáticamente, a una aplicación de red vulnerable. Lo anterior permite al atacante obligar al navegador de la víctima a generar solicitudes ilegítimas, aun cuando la aplicación vulnerada las tenga como legítimas.

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

A partir del marco conceptual esbozado se advierte que los usuarios del sistema de banca electrónica aún enfrentan

[39] Las cookies son archivos de texto con pequeños datos, como un nombre de usuario y una contraseña, que se utilizan para identificar su computadora mientras se utiliza una red informática. Las cookies específicas conocidas como cookies HTTP se utilizan para identificar usuarios específicos y mejorar su experiencia de navegación de la red. El navegador almacena cada mensaje en un archivo pequeño, llamado cookie.txt.; así, al abrir una página en el servidor, su navegador envía la cookie de vuelta, por lo que estos archivos suelen contener información sobre su visita a la página, así como cualquier información que haya proporcionado voluntariamente, como su nombre e intereses. Recuperado de la Universidad de Indiana (Indiana University), en la liga electrónica siguiente: "*https://kb.iu.edu/d/agwm*"

dificultades en relación con el acceso no autorizado a sus cuentas bancarias.

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

Existen alrededor del mundo diversos ejemplos de vulneraciones en la ciberseguridad de las instituciones bancarias, ejemplo de ello, lo constituye el robo masivo suscitado en el Reino Unido respecto de Tesco Bank en noviembre de dos mil dieciséis, quien sufrió una violación de seguridad en línea en la que se retiraron un total de dos millones y medio de libras esterlinas, de veinte mil de sus ciento treinta y seis mil cuentas corrientes, detectándose actividad sospechosa sobre un porcentaje similar[40].

Nuestro país no es la excepción[41]. En dos mil dieciocho, el Banco de México reportó que piratas informáticos robaron alrededor de trescientos millones de pesos al crear órdenes fantasmas para transferir fondos a cuentas falsas para luego retirarlos. Lo anterior ocurrió mediante un ciberataque al software aplicativo usado por algunos bancos para conectarse al SPEI, lo que afectó las transferencias electrónicas, confirmándose la realización de operaciones no autorizadas[42].

---

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

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

[42] Caso SPEI: la cronología del hackeo al sistema financiero mexicano. Recuperado de: "https://expansion.mx/economia/2018/05/18/caso-spei-la-cronologia-del-hackeo-al-sistema-financiero-mexicano."

Al respecto, cabe destacar que el propio Banco de México ha reconocido que la violación de seguridad ocurrió en la etapa previa a la valoración de formato en la plataforma SPEI, es decir, en la etapa de instrucción de pago y firma digital del banco participante; empero, lo cierto es que, con independencia del momento específico que se haya suscitado el ataque, a partir de su actualización, se logró evidenciar la existencia de nuevas y más eficientes tecnologías para llevar a cabo ciberataques. [43]

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

Para ello se ha recomendado no solo la implementación de métodos que incluyan el uso de contraseñas y números de identificación, certificados digitales, contraseñas de un solo uso y otros tipos de “tokens”, pues el nivel de protección contra riesgos que ofrece cada una de estas técnicas varía, por lo que es aconsejable adoptar la implementación de diferentes y más novedosas técnicas como podrían ser las características biométricas de los usuarios. Al respecto el Consejo Examinador de Instituciones Financieras Federales (Federal Financial Institutions Examination Council FFIEC), establece que las metodologías de autenticación deben involucrar tres factores básicos: a) algo que el usuario sepa (por ejemplo, contraseña, PIN); algo que el usuario tenga (verbigracia, una tarjeta bancaria); y, algo que sea del usuario (por ejemplo, características biométricas como una huella dactilar, el iris ocular o el reconocimiento facial).[44]

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

Precisamente, ante la presencia de estos riesgos, las autoridades han ido adecuando la normatividad aplicable a las instituciones financieras para prever obligaciones específicas en cuanto al establecimiento de mecanismos reactivos y/o preventivos para combatir las prácticas irregulares que

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

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

pretendan obtener un provecho ilegitimo por medio de la vulneración a estos sistemas electrónicos.

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

De manera general, la Ley de Instituciones de Crédito en su artículo 52 establece que las instituciones de crédito podrán pactar la celebración de sus operaciones y la prestación de servicios con el público mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, en donde se establecerá con claridad los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.

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

De manera particular, la Comisión Nacional Bancaria y de Valores, al emitir las Disposiciones de Carácter General aplicables a las Instituciones de Crédito[45], estableció un

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

capítulo específico por lo que se refiere a la operación de la banca electrónica, dentro del Título Quinto denominado “Otras disposiciones”.

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

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

Tratándose de trasferencias de recursos dinerarios a cuentas destino de terceros u otras instituciones, el artículo 313 del ordenamiento en comento exige que dicha operación sea precedida de un factor de autenticación de categorías 3 o 4, no solo para iniciar la sesión en la cuenta bancaria, sino en cada ocasión que se pretenda realizar ésta. En términos del artículo 310 estas categorías comprenden lo siguiente: la categoría 3 se compone de información contenida, recibida o generada por medios o dispositivos electrónicos, así como la obtenida por dispositivos generadores de contraseñas dinámicas de un solo uso; por su parte, la categoría 4 corresponde a la información del usuario derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano, patrones en iris o retina y reconocimiento facial, entre otras.

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

diciembre de 2014, 9 de enero, 5 de febrero, 30 de abril, 27 de mayo, 23 de junio, 27 de agosto, 21 de septiembre, 29 de octubre, 9 y 13 de noviembre de 2015, respectivamente.

De esta manera, en el artículo 314 se dispone que para la celebración de las operaciones monetarias como lo es la transferencia de recursos dinerarios, las cuentas de destino deben registrarse de forma previa a que se realicé la trasferencia de dinero; precisándose en el párrafo quinto del precepto citado que, salvo algunas excepciones cono las que se registren a través de la Banca Móvil[46], "(…) *las cuentas de destino deberán quedar habilitadas después de un periodo determinado por la propia institución; sin que este sea menor a treinta minutos contados a partir de que se efectué el registro*". Asimismo, en el párrafo sexto se prevé que "*(…) las Instituciones puedan] habilitar Cuentas Destino registradas por sus Usuarios sin que les sea aplicable el periodo mínimo de tiempo referido en el párrafo anterior, siempre y cuando sea para la realización de Operaciones Monetarias a través de Banca por Internet cuyo monto agregado diario no exceda al equivalente en moneda nacional a las de Baja Cuantía, o bien, el equivalente en moneda nacional a 1,000 UDIs mensuales y obtengan la previa autorización de la Comisión*."

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

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

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

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

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

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

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

Las Instituciones podrán Desbloquear el uso de Factores de Autenticación que previamente hayan sido Bloqueados en los casos contemplados en las fracciones I y II anteriores, para lo cual podrán utilizar un Factor de Autenticación Categoría 1 a que se refiere el artículo 310 de las presentes disposiciones, en términos de lo previsto por la fracción III del Artículo 312 de estas disposiciones, o bien, realizar a sus Usuarios preguntas secretas, cuyas respuestas deben conservarse almacenadas en forma Cifrada. Para efectos de lo previsto en el presente párrafo, se entenderá por pregunta secreta al cuestionamiento que define el Usuario o la Institución durante el

proceso de contratación del servicio de Banca Electrónica, respecto del cual se genera información como respuesta. Cada pregunta secreta que se defina únicamente podrá ser utilizada en una ocasión.

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

[Énfasis añadido]

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

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

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

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

*Que es conveniente **actualizar los mecanismos para la identificación de los clientes** de las instituciones*

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

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

[Énfasis añadido]

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

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

Con base en lo anterior, y en la línea de lo que esta Primera Sala señaló al resolver la Contradicción de Tesis 128/2018, la presunción en el sentido de que las transferencias mediante mecanismos electrónicos son infalibles, y por ende, que debe trasladarse la carga de la prueba al usuario del servicio bancario, no puede actualizarse en atención a que como ha quedado de manifiesto, actualmente se conocen diversas maneras de poder obtener fraudulentamente datos de los clientes o vulnerarse contenido electrónico para realizar operaciones fraudulentas; de ahí que la institución bancaria es quien debe de acreditar que los procedimientos de identificación que fueron utilizados durante la transacción y que fueron acordados con el usuario fueron emitidos correctamente, además de la fiabilidad del procedimiento que se utilizó para autorizar la transacción, máxime si consideramos que el banco cuenta con la infraestructura para generar la evidencia presentada ante los órganos jurisdiccionales.

e) Conclusión.

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

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

De ahí que, cuando resulte controvertida la validez de una transacción que tenga por objeto la trasferencia de recursos dinerarios a cuentas de terceros u otras instituciones bancarias, no basta con la acreditación de que se introdujeron las claves o contraseñas para acceder al sistema electrónico, con independencia de la categoría que les correspondiera; sino que la institución bancaria deberá demostrar que dicha

operación cumplió igualmente con el procedimiento previsto en las Disposiciones de carácter general aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores, concretamente, que el mecanismo de autenticación correspondía al de la cuantía y formato de la operación, la emisión del comprobante y notificación al usuario de la operación respectiva, el debido seguimiento de los plazos establecidos para el registro de una cuenta destinataria, entre otros que se puedan advertir de las disposiciones antes citadas, según corresponda al monto y canal por el que se lleve a cabo la operación.

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

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

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

De modo que, en las circunstancias concretas, la carga de la prueba implique que sea la parte que ostenta una posición dominante en la relación de consumo la que deba acreditar el

funcionamiento en las condiciones debidas. Siendo que la tecnicidad de los sistemas digitales por medio de los cuales se presta el servicio de la banca electrónica representaría un obstáculo excesivo a efecto de que el usuario del servicio pudiera demostrar su pretensión. A diferencia de ello, las instituciones prestadoras del servicio de banca electrónica se encuentran obligadas a contar con la infraestructura y profesionalización en términos del artículo 316 bis 18 de las Disposiciones de mérito.[47]

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

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

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

"Artículo 316 Bis 15.- *Las Instituciones deberán generar registros, bitácoras, huellas de auditoría de las operaciones y servicios bancarios realizados a través de Medios Electrónicos y, en el caso de Banca*

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

Telefónica Voz a Voz, adicionalmente grabaciones de los procesos de contratación, activación, desactivación, modificación de condiciones y suspensión del uso del servicio de Banca Electrónica, debiendo observar lo siguiente:

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

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

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

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

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

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

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

II. Deberán contar con mecanismos para que la información de los registros de las bitácoras en los diferentes equipos críticos de cómputo y

telecomunicaciones utilizados en las operaciones de Banca Electrónica sea consistente.

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

[Énfasis añadido]

Desde esta perspectiva, en que el consumidor se encuentra en una posición de desventaja frente al prestador del servicio bancario en línea, al no contar con los mecanismos tecnológicos necesarios a los que sí puede acceder la institución bancaria; debe agregarse la resistencia que esta última podría poner cuando se ofreciera alguna prueba por parte del cliente, a fin de revisar la estructura y conformación de sus servidores, pues no debemos perder de vista que dicha data sensible se encuentra bajo un resguardo riguroso al que no puede tener acceso cualquier persona.

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

De ahí que, se insiste, la mera exhibición del registro en que se advierta la operación cuestionada, en ausencia de elementos que permitan verificar que se cumplieron con los protocolos establecidos no se estima suficiente para acreditar

la validez de la transacción. Siendo que si la institución bancaria tuviere conocimiento de cualquier incidente que pudiera haber comprometido los datos del cuentahabiente, así deberá declararlo.

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

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

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

Ello, pues resulta evidente que los servicios financieros a que se hace referencia, encuadran en una relación de consumo en que los usuarios del servicio tienen la calidad de consumidores, y las instituciones bancarias la calidad de proveedoras del servicio. De manera tal que, si bien la protección de los usuarios encuentra su cauce en una legislación especial, estos no pierden su calidad de consumidores, ni la protección multifacética que les asiste en términos del artículo 28 de la Constitución Política de los

Estados Unidos Mexicanos. Alcance que se extiende a todas las vertientes en que pueda llegar a derivar una relación de consumo, como lo es la reivindicación de sus derechos en la vía judicial. Así, la diferencia formal en la protección de los derechos de los usuarios del servicio financiero, no pueda llegar a excluir, *a priori*, los principios y garantías establecidos en favor de los consumidores en general.

Sobre este aspecto, resulta relevante señalar que esta Primera Sala se pronunció al resolver el juicio de amparo directo en revisión 5771/2015[48], en que estableció que la protección de los consumidores no es exclusiva del ámbito administrativo; sino que ésta incluye otras vertientes como son la civil y la mercantil, en tanto que, las relaciones de consumo se sirven de instrumentos normativos e instituciones jurídicas de naturaleza civil y/o mercantil para adoptar una estructura e identidad jurídicas, pero siempre quedan sometidas (en mayor o menor medida) al régimen especial de protección al consumidor que el texto constitucional establece para ese tipo especial de relación derivada del acto de consumo y del rol de consumidor [...]".[49]

Tales consideraciones se hacen propias plenamente en esta ejecutoria, y de ellas derivó la jurisprudencia **1a./J. 17/2021 (10a.)**,[50] del contenido siguiente:

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

Hechos: Los Tribunales Colegiados de Circuito contendientes sostuvieron posturas distintas respecto a quién correspondía demostrar, en un juicio de naturaleza mercantil, la fiabilidad del mecanismo por el cual se

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

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

[50] Localizable en la Gaceta del Semanario Judicial de la Federación, Undécima Época, Libro 1, mayo de 2021, Tomo II, página 1752, registro 2023157.

efectuaron transferencias electrónicas de recursos mediante la utilización de plataformas digitales; así, uno estimó que cuando el cuentahabiente niega haber dado su autorización al banco para realizar la transferencia y la institución de crédito afirma que sí recibió la instrucción, corresponde al primero demostrar que el sistema que opera las firmas electrónicas carece de fiabilidad y, por tanto, que su cuenta fue saboteada electrónicamente; mientras que el otro sostuvo lo contrario, es decir, que corresponde a la institución bancaria soportar la carga probatoria de acreditar que las mismas se realizaron mediante el uso de los elementos de seguridad empleados para garantizar la certeza de las operaciones.

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

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

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

De la jurisprudencia y ejecutoria transcrita, en lo interesante para el caso, se desprende que **no puede presumirse la fiabilidad de la banca electrónica a partir de la mera acreditación de que una transferencia se llevó a cabo utilizando un determinado mecanismo de autenticación por parte del usuario**, como pueden ser “*contraseñas y números de identificación, certificados digitales, contraseñas de un solo uso y otros tipos de tokens”*, porque cada vez existen nuevas y más eficientes tecnologías

para llevar a cabo ciberataques, en donde se cometen fraudes electrónicos y se roba la identidad del cuentahabiente, por lo cual se ha recomendado no sólo la implementación de métodos que incluyan el uso de contraseñas y números de identificación, certificados digitales, contraseñas de un solo uso y otros tipos de "tokens", pues el nivel de protección contra riesgos que ofrece cada una de estas técnicas varía, por lo cual se aconseja adoptar la implementación de diferentes y más novedosas técnicas como podrían ser las características biométricas de los usuarios e, incluso, se destacó que el Consejo Examinador de Instituciones Financieras Federales (Federal Financial Institutions Examination Council FFIEC), establece que las metodologías de autenticación deben involucrar tres factores básicos: a) algo que el usuario sepa (por ejemplo, contraseña, PIN); algo que el usuario tenga (verbigracia, una tarjeta bancaria); y, algo que sea del usuario (por ejemplo, características biométricas como una huella dactilar, el iris ocular o el reconocimiento facial).

Además, la superioridad fue explícita en indicar que los grupos delictivos, después de robar la identidad de los cuentahabientes, **usan sus claves o información confidencial "*para autenticar transacciones fraudulentas*"; de ahí la importancia de no dar por válida una transacción por el solo hecho de haber sido utilizados factores de autenticación.**

Por tanto, concluyó que: *"cuando resulte controvertida la validez de una transacción que tenga por objeto la trasferencia de recursos dinerarios a cuentas de terceros u*

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

Ahora, el hecho de que la dirección IP desde la cual se originó la transacción impugnada corresponda a un área geográfica de Israel, por sí mismo, **acredita de forma contundente la deficiencia de los mecanismos de seguridad del sistema de banca electrónica de la enjuiciada**, por incumplimiento de las Disposiciones de carácter general aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores.

Ello, porque de los numerales 316 bis 2, fracción I, inciso b, 316 bis 13 y 316 bis 15, fracción I, inciso d) de dicho ordenamiento, se desprende que las instituciones de crédito, como la aquí quejosa, deberán proveer lo necesario para que una vez autenticado el usuario en el servicio de banca

electrónica de que se trate, la sesión no pueda ser utilizada por un tercero y que, para efectos de lo anterior, las instituciones deberán establecer, al menos, los mecanismos siguientes: dar por terminada la sesión en forma automática, e informar al usuario del motivo en el caso de que en el curso de una sesión del servicio de banca por internet, la institución identifique cambios relevantes en los parámetros de comunicación del medio electrónico, tales como identificación del dispositivo de acceso, "rango de direcciones de los protocolos de comunicación, ubicación geográfica, entre otros"; asimismo, las instituciones están facultadas para detectar y prevenir eventos apartados de los parámetros de *"uso habitual"* de los usuarios, como suspendiendo la utilización del servicio de Banca Electrónica o, en su caso, de la operación que se pretenda realizar (lo que implica rechazarla), en el evento de que cuenten con elementos que hagan presumir que el identificador de usuario o los factores de autenticación no están siendo utilizados por el propio usuario; igualmente, que en la bitácoras generadas de su parte, las instituciones de crédito deberán registrar las direcciones de los protocolos de internet o similares; ello, tal como se advierte de la siguiente transcripción

> "Artículo 316 Bis 2.- Las Instituciones deberán proveer lo necesario para que una vez autenticado el Usuario en el servicio de Banca Electrónica de que se trate, la Sesión no pueda ser utilizada por un tercero. Para efectos de lo anterior, las Instituciones deberán establecer, al menos, los mecanismos siguientes:
> I. Dar por terminada la Sesión en forma automática, e informar al Usuario del motivo en cualquiera de los casos siguientes:
> [...]

b) Cuando en el curso de una Sesión del servicio de Banca por Internet, la Institución identifique cambios relevantes en los parámetros de comunicación del Medio Electrónico, tales como identificación del Dispositivo de Acceso, rango de direcciones de los protocolos de comunicación, ubicación geográfica, entre otros".

Artículo 316 Bis 13.- Las Instituciones deberán mantener mecanismos de control para la detección y prevención de eventos que se aparten de los parámetros de uso habitual de sus Usuarios a través de Medios Electrónicos. Para tales efectos, las Instituciones podrán:

I. Solicitar a sus Usuarios la información que estimen necesaria para definir el uso habitual que estos hagan de los servicios de Banca Electrónica.

II. Aplicar, bajo su responsabilidad, medidas de prevención, tales como la suspensión de la utilización del servicio de Banca Electrónica o, en su caso, de la operación que se pretenda realizar, en el evento de que cuenten con elementos que hagan presumir que el Identificador de Usuario o los Factores de Autenticación no están siendo utilizados por el propio Usuario, debiendo informar a este tal situación de forma inmediata. Lo anterior, en los términos y condiciones que las Instituciones hayan pactado con sus Usuarios en el contrato respectivo.

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

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

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

Cabe precisar que tales preceptos fueron adicionados a las **Disposiciones de Carácter General Aplicables a las Instituciones de Crédito** publicadas en el Diario Oficial de la Federación el dos de diciembre de dos mil cinco, mediante reforma difundida en ese mismo medio de comunicación el veintisiete de enero de dos mil diez,[51] por lo cual, eran de observancia obligatoria para la aquí peticionaria al momento en que se realizó la transacción impugnada, el treinta de mayo de dos mil dieciséis.

Así, el hecho de que el protocolo o dirección de internet IP desde la cual se originó la operación cuya nulidad se pretende, de número **31.168.172.139**, corresponda a un área geográfica de Israel, cuando el domicilio principal de la actora registrado en el contrato bancario está ubicado en México, y el objeto de dicha operación haya sido la transferencia de miles de pesos, ante los ojos de cualquier observador racional, constituye **una actividad inusual que ameritaba, por precaución básica, dar por terminada la sesión de forma automática y suspender la utilización del servicio de banca electrónica o la operación o rechazarla directamente, con base en la interpretación armónica y aplicación de los numerales 316 bis 2, fracción I, inciso b y 316 bis 13 de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores**.

De este modo, el hecho de que la operación impugnada se haya originado desde esa IP de Israel (sea porque quien

[51] Disponible desde internet en: https://www.cnbv.gob.mx/Resoluciones%20Modificatorias/23a.%20Resoluci%C3%B3n%20modificatoria%20CUB.pdf

robó la identidad haya estado verdaderamente en ese país o haya utilizado un programa para disfrazar su ubicación real a través de ese protocolo), y aun así la ahora peticionaria haya autorizado la transferencia **revela que en el juicio de origen no sólo la aquí quejosa omitió acreditar que siguió los procedimientos establecidos normativamente para acreditar su fiabilidad, sino que por el contrario, quedó demostrada la falta de fiabilidad de sus sistemas electrónicos, pues un dato tan grave y evidente como lo es lo inusual de la ubicación geográfica de la IP de donde procedió la operación, no fue detectado por sus mecanismos de seguridad.**

De ahí que ante la apuntada deficiencia en los filtros de seguridad de la quejosa en la prestación del servicio de banca electrónica, no puede considerarse que la actora otorgó su consentimiento en la operación impugnada, a pesar de que se pudieran o no haber utilizado todos los datos de autenticación de la accionante, como lo pueden ser nombres de usuarios, claves, claves dinámicas derivadas de tokens o netkey, o cualquier otro factor de autenticación, pues como lo estableció la Primera Sala de Suprema Corte de Justicia de la Nación, de forma obligatoria en términos del numeral 217 de la Ley de Amparo "*no basta con la acreditación de que se introdujeron las claves o contraseñas para acceder al sistema electrónico, con independencia de la categoría que les correspondiera; sino que la institución bancaria deberá demostrar que dicha operación cumplió igualmente con el procedimiento previsto en las Disposiciones de carácter general aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores"*; ello, pues no se

siguieron los procedimientos establecidos en los numerales 316 bis 2, fracción I, inciso b y 316 bis 13 de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores.

Así, en oposición a lo argumentado por la quejosa, el hecho de que la IP de donde se originó la transacción impugnada corresponda al área geográfica de Israel no es "intrascendente", sino todo lo contrario, pues se trata de un dato inusual indicativo de posible robo de identidad o de datos de autenticación que debió activar los sistemas de seguridad del banco a fin de evitar cualquier intento de fraude en contra de la accionante, en los términos de la normatividad indicada, y el hecho de que el perito tercero en discordia pudiera o no haber contestado que la operación se realizó desde un dispositivo celular, o que ésta pudo efectuarse en cualquier parte del mundo siempre y cuando se conocieran los datos de autenticación de la accionante, no eximía a la institución bancaria de activar los mecanismos de seguridad correspondientes pues, se enfatiza, el hecho de que la banca electrónica permita realizar transacciones en cualquier lugar no le quita la naturaleza inusual a la operación, porque la localización de la IP de procedencia correspondiente a un país diverso al domicilio principal del cuentahabiente, aunado al hecho notorio en términos del numeral 88 del Código Federal de Procedimientos Civiles, de que la mayoría de los cuentahabientes nacionales no realizan habitualmente transferencias desde Israel hacia la cuenta de un tercero; de ahí lo ***infundado*** de los conceptos de violación respectivos.

Igualmente, son ***infundados*** la totalidad de los conceptos de violación en los cuales la quejosa asegura que es fiable el sistema de banca electrónica a través del cual se realizó la transacción impugnada porque, con las periciales, quedó demostrado que la plataforma cuenta con cuatro elementos de seguridad: 1) protocolo HTTPS; 2) bloqueo de la cuenta por ingresar firma electrónica falsa; 3) cierre de la sesión por inactividad del usuario dentro del portal; y 4) que solamente se puede tener una sesión por Netkey; así como que lo anterior se complementó con la firma electrónica la cual se compone de tres factores de autenticación: 1) número de cliente; 2) número de identificación personal; y 3) clave aleatoria y dinámica proporcionada por el Netkey; dando así un total de siete variables o elementos que, en conjunto, protegieron la transacción y la volvieron cierta, lo cual asevera fue aceptado por los "*peritos*".

Lo anterior es así, porque incluso en el supuesto no concedido de que fuera verdad que de la información aportada por los peritos se advirtiera que la plataforma contaba con esos cuatro elementos de seguridad, y que la firma electrónica con los otros tres elementos, lo cierto es que quedó acreditado en el juicio que la transacción se originó desde una IP del área geográfica de Israel y aún así se autorizó la operación en flagrante transgresión a los numerales 316 bis 2, fracción I, inciso b y 316 bis 13 de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores, **lo cual evidencia que esos cuatro elementos de seguridad de la plataforma son insuficientes para que sea fiable, en tanto, como lo**

decretó la Suprema Corte de Justicia de la Nación, el hecho de que se pudieran haber utilizado para conformar la firma electrónica las credenciales de la accionante consistentes en el número de cliente; el número de identificación personal; y la clave aleatoria y dinámica proporcionada por el Netkey, no es indicativo de que la accionante otorgó su consentimiento o autorizó la operación, pues ello depende de la demostración de que se siguieron los procedimientos establecidos previamente para acreditar su fiabilidad, lo cual no ocurrió así, pues se vulneraron los procedimientos establecidos en los numerales precitados, lo cual evidencia que los datos de autenticación pudieron utilizarse para tratar de legitimar una operación fraudulenta en perjuicio de la accionante.

Por razones similares, son ***infundados*** los conceptos de violación en los cuales la quejosa afirma repetitivamente que los dictámenes periciales fueron valorados o analizados de forma incompleta, incongruente o poco exhaustiva, bajo el razonamiento que de ellos se desprende que los diestros coincidieron en que era imposible autorizarse la operación impugnada sin los datos de autenticación y que esas credenciales sólo las conoce la accionante, lo cual evidencia la fiabilidad del sistema bancario electrónico.

Lo anterior es así, pues por más que la peticionaria afirme repetitivamente que las claves y dispositivos como el netkey “4” son únicas y sólo tiene acceso a ellas el usuario (a través de sus empleados), lo cierto es que da por sentado que puede acreditarse la fiabilidad de la banca electrónica a

partir de la mera demostración de que una transferencia se llevó a cabo utilizando un determinado mecanismo de autenticación por parte del usuario, a través del uso de claves confidenciales; sin embargo, tal como se mencionó en párrafos previos, para ello no basta con la acreditación de que se introdujeron las claves o contraseñas para acceder al sistema electrónico, con independencia de la categoría que les correspondiera o de quien las detente o le corresponda su resguardo; pues la institución bancaria debe demostrar que dicha operación cumplió igualmente con el procedimiento previsto en las **Disposiciones de carácter general aplicables a las Instituciones de Crédito** emitidas por la Comisión Nacional Bancaria y de Valores, siendo que en el caso quedó demostrado lo contrario, esto es, que la peticionaria incumplió con los procedimientos establecidos en tales disposiciones, concretamente en sus numerales numerales 316 bis 2, fracción I, inciso b y 316 bis 13.

Sin que lo anterior implique obligar a la actora a lo *“imposible”* como argumenta de manera por demás ***infundada*** en sus conceptos de violación, bajo el argumento de *reducción al absurdo* consistente en que para acreditar fehacientemente que la empleada de la accionante tecléo la información tendría que colocar cámaras permanentes para grabar a cada uno de los usuarios de banca electrónica los cuales son decenas de miles, y además de tener a disposición personal del banco en tiempo real para realizar la validación fisionómica de las personas.

Lo anterior es así, pues en la especie no se llega al extremo de imponérsele a la institución financiera la carga de

demostrar la fiabilidad "*abstracta"* del sistema, en los términos sugeridos de su parte, sino simplemente de demostrar haber seguido el procedimiento normativamente exigido ante una eventualidad, concretamente, las Disposiciones de carácter general aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores, siendo que en el caso, quedó evidenciado lo contrario, es decir, que a pesar de la eventualidad constistente en una transferencia con IP procedente de Israel no suspendió el servicio de banca electrónica por seguridad, rechazó la operación, o empleó un mecanismo análogo para evitar un fraude en términos de los numerales 316 bis 2, fracción I, inciso b y 316 bis 13 del ordenamiento citado, a pesar de provenir la solicitud de una ubicación geográfica a todas luces inusual; lo cual, de manera alguna supone una carga imposible, como la hipótesis de colocar una cámara a cada cuentahabiente, sino en todo caso la carga de respetar la normatividad y crear o mejorar sus mecanismos de defensa informáticos para poder detectar ese tipo de operaciones con IP inusuales a fin de ser rechazadas efectivamente.

Igualmente son ***infundados*** los conceptos de violación relativos a que fue responsabilidad de la actora el manejo de sus contraseñas y la información confidencial, y que su vulneración no puede deparar perjuicio al banco; lo anterior, pues esos señalamientos se basan en una premisa no demostrada consistente en que la accionante reveló intencionalmente y libre de todo engaño *(sic)* su información confidencial a terceros, lo cual demerita por sí solo al planteamiento, aunado a que la posibilidad de que sea necesario una mejor capacitación del *"eslabón más débil de*

la cadena que es el usurario", quien consciente o inconscientemente al caer víctima de técnicas de ingeniería social como pishing (correos falsos), vishing (llamadas telefónicas falsas), pharming (páginas web falsas), smishing (mensajes de texto falsos), entre otras, puede llevar a compartir su información, no libera a la institución de crédito de cumplir con la normativa bancaria ante el caso de operaciones con origen en IP's con ubicaciones inusuales, pues es su obligación observarla con independencia de la actitud asumida por el cuentahabiente; siendo que en el caso sí hay prueba de que la seguridad del banco fue vulnerada o resultó insuficiente, pues quedó demostrado en juicio que validó una operación proveniente de una dirección de internet de Israel solicitando la transferencia de recursos, a lo que pretende restarle importancia por haber sido utilizados todos los factores de autenticación procedentes, siendo que esto último, como lo indicó la Suprema Corte de Justicia de la Nación en jurisprudencia obligatoria, no hace presumir la fiabilidad del sistema, ante la existencia de nuevas y más eficientes tecnologías para llevar a cabo ciberataques.

Incluso, en la precitada contradicción de tesis 206/2020, la Primera Sala de la Suprema Corte de Justicia de la Nación destacó que en dos mil dieciocho, el Banco de México reportó que piratas informáticos robaron alrededor de trescientos millones de pesos al crear órdenes fantasmas para transferir fondos a cuentas falsas para luego retirarlos. Lo anterior ocurrió mediante un ciberataque al software aplicativo usado por algunos bancos para conectarse al SPEI, lo cual afectó las transferencias electrónicas, confirmándose la realización

de operaciones no autorizadas;[52] **de ahí la imposibilidad de aceptar la presunción de la fiabilidad del sistema por haberse utilizado los factores de autenticación en la operación impugnada.**

Ahora, el hecho de que en su dictamen el perito tercero en discordia haya o no insertado impresiones de pantalla sobre las recomendaciones que el banco realiza para evitar fraudes tampoco libera a dicha institución de cumplir con sus obligaciones normativas ni acredita la fiabilidad del sistema, pues con independencia de ello, la institución de crédito está obligada a observar las disposiciones normativas sobre seguridad repectivas; de ahí que tal circunstancia no pueda constituir una incongruencia pericial, como tampoco, se enfatiza, que se haya señalado al usuario como el eslabón más *"débil"*, pues precisamente esta circunstancia refuerza la idea aquí sostenida de que las instituciones de crédito están obligadas a acatar estrictamente lo dispuesto en la normatividad correspondiente, por ser los expertos por excelencia en la materia y no los usuarios.

Lo anterior, en la inteligencia de que contrario a lo afirmado repetitivamente por la quejosa, el perito tercero en discordia sí demostró una particularidad sobre la vulnerabilidad en el sistema electrónico, consistente en la validación de una operación proveniente de un IP correspondiente al área geográfica de Israel, lo cual implica una transgresión a las Disposiciones de carácter general aplicables a las instituciones de crédito, dada la falta de

[52] Caso SPEI: la cronología del hackeo al sistema financiero mexicano. Recuperado de: "https://expansion.mx/economia/2018/05/18/caso-spei-la-cronologia-del-hackeo-al-sistema-financiero-mexicano."

demostración de reacción en los términos normativos ante tal suceso por parte del banco; de ahí que el sentido de la sentencia reclamada haya sido **objetivamente correcto, y no dogmático, obtuso, ilegal, incongruente, transgresor de los principios de exhaustividad, de impartición de justicia, de debida fundamentación y motivación, y demás adjetivos similares pronunciados de manera por demás repetitiva, indiferenciada y desarticulada por parte de la peticionaria.**

Por otra parte, a diferencia de lo argumentado de forma ***infundada*** por la quejosa, se enfatiza, la circunstancia de que el perito tercero en discordia pudiera haber dictaminado que el banco sí implementa diversas medidas de seguridad, como alertas de fraudes electrónicos, el protocolo HTTPS, las herramientas anti-intruso, el sistema de suspensión por acceso incorrecto en más de tres ocasiones a la banca electrónica, por periodo de inactividad, o por utilización de un solo netkey; así como que haya indicado que sí se utilizaron los factores de autenticación de la actora y que bajo la perspectiva de esos elementos la operación haya sido *"legímita"* tal como se advierte de la respuesta a la pregunta 48 del cuestionario, **no se traduce en que la accionante haya sido realmente quien autorizó la operación**, pues como se indicó con antelación, si la fiabilidad del sistema de banca electrónica no se constató mediante la demostración del seguimiento de los procedimientos establecidos normativamente para acreditar su fiabilidad, la autenticación de factores no equivale al consentimiento, lo cual incluso fue destacado por el perito al dar respuesta a dicha interrogante:

> "[...] Bajo esa óptica, considero que las transferencias se consideran legítimas en su operación al cumplir con las disposiciones aludidas, más no significa que las haya realizado la actora como lo menciono en las conclusiones de este dictamen".

Cabe indicar que, en tales conclusiones, el perito destacó el hecho de que la dirección IP de donde se realizó la transacción proviene del área geográfica de Israel y que aunque lo datos de autenticación fueron utilizados cabalmente, éstos pudieron obtenerse mediante técnicas o combinación de técnicas de *"ingeniería social" como phishing, vishing, pharming, o smishing, entre otras, realizando con ellas el robo de identidad*; siendo que esto último impide considerar, como lo hace de forma por demás equivocada el banco, que debe concluirse que si se utilizaron las claves confidenciales o credenciales es porque el personal de la accionante las reveló a propósito o porque el personal mismo realizó la transacción de mala fe en perjuicio de la empresa, pues como se indicó con antelación, la institución de crédito no demostró la fiabilidad del sistema, por lo cual, opera una presunción en su contra respecto a que hubo robo de identidad; sin perjuicio de que a criterio de la banca en la audiencia especial el apoderado de la actora haya presentado un netkey distinto al verdadero "número 4" lo que incluso afirma se reconoció en la audiencia *confesional*, y considera debe tener como consecuencia el decretar como presuntivamente ciertos los hechos de la defensa del banco; todo lo cual carece de sustento, **pues el ámbito demostrativo de ese netkey, en todo caso, se vincula con la utilización o no de las claves y contraseñas a resguardo de la accionante como factor de autenticación,**

pero su exhibición oportuna o no carece de impacto directo en la demostración de la fiabilidad del sistema de banca electrónica frente a operaciones provenientes de IP's inusuales, lo cual va más allá de la utilización de factores de autenticación, siendo el origen de esa dirección IP la razón toral en la cual se fincó el sentido del acto reclamado.

Por otra parte, el hecho de que el banco haya cumplido con algunas estrategias de seguridad no la eximía de implementar el resto de medidas idóneas para prevenir operaciones provenientes de IP's inusuales, pues los procedimientos establecidos en los numerales 316 bis 2, fracción I, inciso b y 316 bis 13 de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores, no prevén la posibilidad de ser intercambiables por otro tipo de medidas de seguridad que le son impropias, como lo son, por ejemplo, el protocolo HTTPS, el sistema de suspensión por acceso incorrecto en más de tres ocasiones, o los anuncios a manera de alertas contra fraudes, que no son idóneas para neutralizar una operación fraudulenta cuya nota distintitiva es la ***ubicación geográfica de su origen*** y que ***está en curso a través de los factores correctos de autenticación***.

Por otra parte, **contrario a lo aseverado por la quejosa**, la autoridad responsable no ignoró elementos relevantes del dictamen emitido por el perito tanto del propuesto de su parte como del tercero en discordia, pues el primero encaminó su estudio a tratar de convencer de que los factores de autenticación fueron utilizados de manera

correcta, lo cual es irrelevante si no se comprueba que se siguieron los procedimientos establecidos normativamente para acreditar su fiabilidad, de ahí el ser inatendible para los propósitos de la litis en la parte relativa a la fiabilidad del sistema; en cambio, a la luz de los numerales 316 bis 2, fracción I, inciso b y 316 bis 13 de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores, el segundo diestro si proporcionó elementos técnicos para determinar si se siguieron tales procedimientos normativos, al exponer que la IP procede del área geográfica de Israel, que ello se debe a que quien realizó la transacción se encontraba en ese lugar o utilizó un programa para evitar ser rastreado y aparentar informáticamente estar ahí, y aunque se utilizaron los factores de autenticación, esto pudo deberse al robo de identidad mediante técnicas de ingeniería social como pishing (correos falsos), vishing (llamadas telefónicas falsas), pharming (páginas web falsas), smishing (mensajes de texto falsos), entre otras.

Dicho de otro modo, el experto detalló qué es una IP, a qué ubicación geográfica corresponde la vinculada con la transacción impugnada, cuáles son las dos posibilidades por las que apareció como dirección de origen Israel, y de qué manera pudo obtenerse la información confidencial de la actora, a pesar de encontrarse en un lugar distinto a aquel país, lo cual es lógico y coherente, por carecer de premisas contradictorias entre sí y, más aún, reforzarse unas con otras para generar premisas sólidas de una conclusión alcanzada por un profesional en la materia de Ingeniería en Comunicaciones y Electrónica, quien al comenzar con

dictamen anticipó que utilizaría el método científico, auxiliado del deductivo y comparativo, para formar su opinión, los cuales no se tiene noticia que hayan sido superados por su especialidad, y efectivamente procedió conforme a esos cánones, pues sustentó sus señalamientos en conocimientos propios de su ciencia y no en conceptos dogmáticos bajo señalamientos carentes de comprobación alguna.

De ahí que conforme a las normas de la sana crítica, de la lógica y de la experiencia, se comparte lo decidido por el juez responsable en cuanto a conceder fuerza probatoria al dictamen emitido por el perito tercero en discordia en el aspecto aquí destacado de la litis, por su coherencia y por aportar elementos relacionados con la fiabilidad del sistema electrónico en la vertiente de interés, apegados al sentido común y a la lógica de los acontecimientos y, por ende, el acto reclamado no violó el numeral 1301 del Código de Comercio, en los términos pretendidos por la disidente;[53] máxime que la quejosa es dogmática en sus planteamientos, pues no precisa qué respuestas precisas recaídas a cuestionamientos y preguntas hechas al perito ofrecido de su parte le favorecen y desvirtúan el tema relativo al origen de la dirección IP, por lo cual no consolida la causa de pedir, pues se trata de un asunto de estricto derecho en donde este Tribunal no puede emprender el análisis de probanzas a partir de señalamientos de naturaleza inacabada.

Así, no favorecen a la quejosa las tesis citadas de su parte, de rubros: ***“PRUEBA PERICIAL EN EL JUICIO MERCANTIL. EL ARTÍCULO 1301 DEL CÓDIGO DE***

[53] Art. 1,301. La fe de los demás juicios periciales, incluso el cotejo de letras, será calificada por el juez según las circunstancias.

COMERCIO NO VIOLA EL DEBIDO PROCESO EN SU VERTIENTE DEL DERECHO A LA PRUEBA” y ***“PRUEBA PERICIAL. SU VALORACIÓN EN EL JUICIO DE AMPARO”***.

Por su parte, son ***inoperantes*** la totalidad de los conceptos de violación en los que la peticionaria afirma que la autoridad responsable omitió tomar en consideración las siguientes probanzas ofrecidas de su parte:

a) Documental privada. Consistente en las copias certificadas en términos del artículo 100 de la Ley de Instituciones de Crédito, respecto de la **“solicitud única *******”**, la cual se encuentra firmada por la parte actora.

b) Documental pública. Consistente en las copias certificadas en términos del artículo 100 de la Ley de Instituciones de Crédito, de la **impresión de pantalla** de los sistemas electrónicos de la demandada titulado **“******* Medios de Entrega Electrónicos, Banca Electrónica, Consulta Específica de Transacción”**, que contiene el registro de la operación materia de la controversia,

c) Documental pública. Consistente en la copias certificadas en términos del artículo 100 de la Ley de Instituciones de Crédito de la **Impresión de Pantalla de los Sistemas Electrónicos de la enjuiciada que contienen los registros titulados como “Sistema 500 (movimientos por contrato); sistema 015 (movimientos de Bca. Elec. Cargo y abono) y clientes operativo bitácora histórica Monterrey *(sic)*.**

d) Documental privada. Consistente en las copias certificadas en términos del artículo 100 de la Ley de Instituciones de Crédito, respecto de la **impresión de la pantalla** proveniente de los sistemas electrónicos del banco, titulada como **"sistema de clientes, representantes del cliente para banca digital"**, el cual contiene la relación de los Netkey proporcionados a la parte actora para operar dentro de la banca electrónica y de las cuales se puede apreciar el número de identificador de cada uno, en especial el número cuatro que fue otorgado para el uso operativo de ***** ******** *******.

e) Documental privada. Consistente en las copias certificadas en términos del artículo 100 de la Ley de Instituciones de Crédito, respecto de la **impresión de la pantalla proveniente de los sistemas electrónicos del banco, titulada como *"sistema de clientes, cuentas para pagos/cargos a terceros"*,** la cual contiene el registro de la fecha del alta de la cuenta de destino de los recursos materia de la transacción impugnada.

f) Documental pública. Consistente en las copias certificadas de la escritura pública ****** de treinta y uno de enero de dos mil dieciocho, que contiene el poder otorgado por el banco a favor de los funcionarios quienes suscribieron las certificaciones existentes en los documentos aportados como prueba.

Tales documentales, al no haber sido objetadas, según la quejosa, merecen valor probatorio pleno, en términos de los numerales 100 de la Ley de Instituciones de Crédito y

1247, 1250 y 1296 del Código de Comercio, para acreditar lo siguiente:

1) La relación contractual;

2) La existencia de la instrucción del cliente para ellas *(sic)* al haber coincidido los medios de autenticación y la firma electrónica en base al código numérico;

3) Que las operaciones quedaron registradas y son consultables en forma posterior, su fecha, hora, cuenta de destino institución donde obra dicha cuenta, el importe de las mismas;

4) Que se atribuyen a la hoy actora por contener su número de cliente, demostrando con ello la procencia de cada una de ellas;

5) Que fue la operación autorizada con la firma electrónica correspondiente al operador número 4, ***** ******** *******;

6) El operador quien lo realizó, al igual que la autorización de la operación por cumplirse los medios de autenticación propios de la firma electrónica con la cual se expresa digitalmente el consentimiento y la voluntad del cliente para su ejecución;

7) El número de identificador de cada uno, en especial, el número cuatro que fue otorgado para el uso operativo de ***** ******** *******;

8) El registro de la fecha de alta de la cuenta de destino de los recursos materia de la transacción impugnada en el presente juicio;

9) De acuerdo con lo anterior, la institución de crédito no solamente demostró la existencia de los registros, sino que **existió la presencia de la firma electrónica para realizar transferencias de la actora e incluso el nombre de la persona a la cual estaba registrada la firma** por el número de Netkey utilizado y que es el de la empleada de la actora ***** ******** *******.

Agrega la quejosa que conforme a lo resuelto en el propio acto reclamado ello debió de haber sido valorado por el juez de instancia y, sin embargo, no aconteció así, porque al momento de decidir la controversia olvidó como influencia determinante para el sentido de la sentencia observar que él mismo le otorgó valor probatorio a tales documentos, lo cual implica que debió de haber tenido por acreditadas las excepciones de la institución de crédito.

Tales motivos de disenso son ***inoperantes*** por fincarse en la falsa premisa de que la juez responsable omitió valorar las pruebas indicadas, cuando en realidad sí lo hizo.

Para comprobarlo basta imponerse de la sentencia reclamada, especialmente de las páginas 40 a 52, para advertir que la juzgadora de origen valoró las probanzas reseñadas previamente, de la siguiente manera:

Pruebas a), b), c), d) y e)*"Medios de convicción que al no haber sido objetados virtud a su naturaleza, merecen valor probatorio pleno en términos del arábigo 100 de la Ley de Instituciones de Crédito, exclusivamente en cuanto a los alcances probatorios que de éstas emanan* (sic)*"*.

Prueba f): "*Medio de convicción que por su naturaleza y al no objetarse, merece pleno valor probatorio para acreditar su contenido, en términos del numeral 1292 del Código de Comercio y se estima eficaz para acreditar la facultad legal de los funcionarios que suscribieron las certificaciones en términos del artículo 100 de la Ley de Instituciones de Crédito"*.

Sirve de sustento a lo anterior, por analogía, la jurisprudencia **2a./J. 108/2012 (10a.)**,[54] emitida por la Segunda Sala de la Suprema Corte de Justicia de la Nación, cuyo rubro y texto son:

> ***"AGRAVIOS INOPERANTES. LO SON AQUELLOS QUE SE SUSTENTAN EN PREMISAS FALSAS.*** *Los agravios cuya construcción parte de premisas falsas son inoperantes, ya que a ningún fin práctico conduciría su análisis y calificación, pues al partir de una suposición que no resultó verdadera, su conclusión resulta ineficaz para obtener la revocación de la sentencia recurrida."*

Con independencia de lo anterior, debe indicarse que en sus conceptos de violación la quejosa confunde el valor probatorio de las pruebas mencionada con su eficacia demostrativa para acreditar lo pretendido.

---

[54] Publicada en el Semanario Judicial de la Federación y su Gaceta, en la página: 1326, Libro XIII, de octubre de 2012, Tomo 3, Décima Época, con registro: 2001825.

El valor probatorio de una prueba se refiere a la cualidad del medio de convicción para acreditar su propio contenido, lo que se sustenta en el "*medio*" de prueba en sí mismo y no en su resultado en relación con la procedencia del fondo de la pretensión del oferente, es decir, el valor probatorio se basa en sus características, particularidades y, de estar previstas sus formalidades en la ley, en su concordancia con los requisitos ahí establecidos para tener valor.

Un ejemplo son los documentos públicos, los cuales, conforme al numeral 1237 del Código de Comercio, son todos aquellos reputados como tales en las leyes comunes (generalmente, se caracterizan por estar su formación encomendada por la ley, dentro de los límites de su competencia, a un funcionario público revestido de la fe pública, y los expedidos por funcionarios públicos, en el ejercicio de sus funciones), y éstos, en términos del artículo 1292 del mismo ordenamiento "*hacen prueba plena*"; así, todo documento público, de cumplir con el requisito de haber sido expedido por un funcionario público en ejercicio de sus funciones, o haber estado su formación encomendada a uno con fe pública, por su valor entendido esto como "*validez*", probará plenamente la existencia de su contenido, por haber certeza en su preparación, pero no significará el éxito de la pretensión litigiosa del oferente, pues ello dependerá del resultado del análisis de ese medio de prueba en función de la litis.

En cambio, la <u>eficacia probatoria o demostrativa</u> de la prueba se vincula exclusivamente con el éxito o efectividad

del medio de prueba para demostrar las pretensiones del oferente, para lo cual, un presupuesto es tener valor probatorio. Así, una prueba con valor probatorio otorga elementos cognitivos e información a partir de la cual se puede derivar la verdad de los hechos en litigio; si esto es así, la prueba además de tener valor probatorio, tendrá eficacia demostrativa.

De igual manera, no todas las pruebas con valor probatorio, incluso pleno, suponen la eficacia demostrativa de los hechos debatidos, pues ello dependerá de su susceptibilidad para aportar elementos positivos para acreditar la pretensión del oferente, y si son negativos o ninguno, evidentemente no habrá tal eficacia. Por tanto, el valor probatorio de una prueba no necesariamente se traducirá en su eficacia demostrativa, pero toda prueba con eficacia demostrativa, siempre tendrá como presupuesto tener valor, pues una prueba carente de esto último, no puede ser efectiva para demostrar la pretensión del oferente.

En apoyo a lo anterior, se cita la tesis **III.2o.C.47 K (10a.)**,[55] sustentada por este Segundo Tribunal Colegiado en Materia Civil del Tercer Circuito, del rubro y texto siguientes:

> ***"PRUEBAS. SU VALOR SE VINCULA CON EL MEDIO DE CONVICCIÓN EN SÍ MISMO EN CUANTO A SU CAPACIDAD DE PROBAR, PERO ELLO NO DETERMINA LA EFICACIA DEMOSTRATIVA PARA ACREDITAR LO PRETENDIDO POR EL OFERENTE.*** *El valor probatorio de una prueba se refiere a la cualidad del medio de convicción para acreditar su propio contenido, lo que se sustenta en el "medio" de*

[55] Publicada Gaceta del Semanario Judicial de la Federación, Décima Época, Libro 77, agosto de 2020, Tomo VI, página 6215, registro 2021914.

prueba en sí mismo y no en su resultado en relación con la procedencia del fondo de la pretensión del oferente, es decir, el valor probatorio se basa en sus características, particularidades y, de estar previstas sus formalidades en la ley, en su concordancia con los requisitos ahí establecidos para tener valor. Un ejemplo son los documentos públicos, los cuales, conforme al numeral 1237 del Código de Comercio, son todos aquellos reputados como tales en las leyes comunes (generalmente, se caracterizan por estar su formación encomendada por la ley, dentro de los límites de su competencia, a un funcionario público revestido de la fe pública, y los expedidos por funcionarios públicos, en el ejercicio de sus funciones), y éstos, en términos del artículo 1292 del mismo ordenamiento "hacen prueba plena"; así, todo documento público, de cumplir con el requisito de haber sido expedido por un funcionario público en ejercicio de sus funciones, o haber estado su formación encomendada a uno con fe pública, por su valor entendido esto como "validez", probará plenamente la existencia de su contenido, por haber certeza en su preparación, pero no significará el éxito de la pretensión litigiosa del oferente, pues ello dependerá del resultado del análisis de ese medio de prueba en función de la litis. En cambio, la eficacia probatoria o demostrativa de la prueba se vincula exclusivamente con el éxito o efectividad del medio de prueba para demostrar las pretensiones del oferente, para lo cual, un presupuesto es tener valor probatorio. Así, una prueba con valor probatorio otorga elementos cognitivos e información a partir de la cual se puede derivar la verdad de los hechos en litigio; si esto es así, la prueba además de tener valor probatorio, tendrá eficacia demostrativa. De igual manera, no todas las pruebas con valor probatorio, incluso pleno, suponen la eficacia demostrativa de los hechos debatidos, pues ello dependerá de su susceptibilidad para aportar elementos positivos para acreditar la pretensión del oferente, y si son negativos o ninguno, evidentemente no habrá tal eficacia. Por tanto, el valor probatorio de una prueba no necesariamente se traducirá en su eficacia demostrativa, pero toda prueba con eficacia demostrativa, siempre tendrá como presupuesto tener valor, pues una prueba carente de esto último, no puede ser efectiva para demostrar la pretensión del oferente.”

De esta manera, las probanzas citadas por la quejosa, al afirmarse de su parte estar certificadas en términos del numeral 100 de la Ley de Instituciones de Crédito y pretendidamente no haber sido objetadas,[56] lo cual así fue asumido por la juzgadora responsable, **sólo significa, en todo caso, que hacen fe "*salvo prueba en contrario, en los juicios respectivos para la fijación de los saldos resultantes de las operaciones*", pero eso no equivale a que tengan eficacia demostrativa plena para acreditar sus excepciones y defensas pues por una parte, ello no es el efecto de la falta de objeción ni de gozar de valor probatorio pleno salvo prueba en contrario, aunado a que, como se indicó con antelación, la eficacia demostrativa dependerá de su susceptibilidad para aportar elementos positivos para acreditar la pretensión del oferente, y si son negativos o ninguno, evidentemente no habrá tal eficacia.**

Siendo que en el caso tales probanzas no aportan elementos positivos para acreditar la pretensión del oferente,

---

[56] "Artículo 100.- Las instituciones de crédito podrán microfilmar o grabar en discos ópticos, o en cualquier otro medio que les autorice la Comisión Nacional Bancaria y de Valores, todos aquellos libros, registros y documentos en general, que obren en su poder, relacionados con los actos de la propia institución, que mediante disposiciones de carácter general señale la Comisión Nacional Bancaria y de Valores, de acuerdo a las bases técnicas que para la microfilmación o la grabación en discos ópticos, su manejo y conservación establezca la misma. Los negativos originales de cámara obtenidos por el sistema de microfilmación y las imágenes grabadas por el sistema de discos ópticos o cualquier otro medio autorizado por la Comisión Nacional Bancaria y de Valores, a que se refiere el párrafo anterior, así como las impresiones obtenidas de dichos sistemas o medios, debidamente certificadas por el funcionario autorizado de la institución de crédito, tendrán en juicio el mismo valor probatorio que los libros, registros y documentos microfilmados o grabados en discos ópticos, o conservados a través de cualquier otro medio autorizado.
Transcurrido el plazo en el que las instituciones de crédito se encuentran obligadas a conservar la contabilidad, libros y demás documentos de conformidad con el artículo 99 de esta Ley y las disposiciones que haya emitido la Comisión Nacional Bancaria y de Valores, los registros que figuren en la contabilidad de la institución harán fe, salvo prueba en contrario, en los juicios respectivos para la fijación de los saldos resultantes de las operaciones a que se refieren las fracciones I y II del artículo 46 de esta Ley".

pues la quejosa asegura que con las pruebas mencionadas se demostró, esencialmente, la relación contractual entre las partes, el registro de la operación impugnada, las instrucciones del cliente, la utilización de los medios de autenticación y la firma electrónica del operador 4 ***** ******** *******, el número del cliente, el consentimiento a través de los medios de autenticación, y el registro de la fecha de alta de la cuenta de destino.

Lo anterior revela que las probanzas en mención, a partir de los manifestado por la quejosa, sólo se vinculan con la pretendida demostración de que en la transacción impugnada se utilizaron todas las claves y factores de autenticación de la actora, otorgado a una de sus operadoras (4), lo cual considera evidencia el consentimiento de la accionante en la transferencia; sin embargo, como se ha explicado previamente, la consideración toral para declarar la nulidad del a operación fue que el IP de la operación corresponde a un área geográfica de Israel, lo cual es independiente a si los factores de autenticación fueron usados o no, **pues la autorización de la transacción en esos términos evidencia la falta de fiabilidad del sistema de seguridad de la banca electrónica y la vulneración de los numerales 316 bis 2, fracción I, inciso b y 316 bis 13 de las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito emitidas por la Comisión Nacional Bancaria y de Valores**.

De ahí que la autoridad responsable no haya incurrido en incongruencia, falta de exhaustividad, ilegalidad u omisión alguna al no conceder eficacia demostrativa a las pruebas en

mención a favor de los intereses de la quejosa, pues carecen de tal calidad para acreditar la fiabilidad del sistema electrónico, dado que quedó demostrado que la dirección IP de donde se realizó la operación corresponde al área geográfica de Israel, sin que la institución bancaria, ante tal situación, haya seguido el procedimiento establecido en la normatividad citada en el párrafo anterior, consistente, entre otras cosas, en la suspensión del servicio de banca electrónica a fin de prevenir un posible fraude o ataque cibernético, a pesar de ser el banco la parte subordinante en la relación de poder frente al usuario, que cuenta con los recursos económicos y la infraestructura suficiente para adoptar medidas de protección adecuadas.

Así, por más que pudiera acreditarse con esas probanzas la utilización de todos los elementos de autenticación, la falta de fiabilidad del sistema impide considerar que la autorización de la transacción se haya dado efectivamente por la peticionaria; de ahí lo objetivamente correcto de decretar la nulidad de la transacción, y que no se hayan transgredido los principios enunciados por la promovente, como el de congruencia, así como la tesis de rubro: ***“PRINCIPIO DE CONGRUENCIA. QUE DEBE PREVALECER EN TODA RESOLUCIÓN JUDICIAL”***, al no conceder eficacia demostrativa a las probanzas indicadas por las razones ya expuestas, siendo entonces coherente la decisión de la autoridad responsable en cuanto a considerar que la validación de la operación proveniente de un IP ubicado en el área geográfica de Israel es un vicio de fiabilidad que impide considerar autorizada la operación impugnada por la verdadera cuentahabiente, más allá de que

se hayan utilizado o no todas sus claves confidenciales o credenciales; asimismo, la sentencia reclamada no carece de fundamentación en tal aspecto, porque al valorar las pruebas materia de inconformidad incluso citó el numeral 100 de la Ley de Instituciones de Crédito, y el artículo 1292 del Código de Comercio.

Sin ser relevante al respecto que, según la quejosa, los peritos no hayan demostrado la falsedad de los documentos correspondientes a las pruebas citadas, pues el hecho de que no se haya desvirtuado su autenticidad no les otorga eficacia demostrativa para el éxito de la pretensión de la inconforme; máxime cuando se vinculan con aspectos que no desvirtúan directamente el hecho de que la IP perteneciente a la operación impugnada tiene origen en el área geográfica de Israel, en lo que recae el vicio de fiabilidad que motivó la declaración de procedencia de la acción.

En tales condiciones, al haber resultado los conceptos de violación principales ***infundados*** en una parte e ***inoperantes*** en otra, y no actualizarse alguna de las hipótesis que justifique suplir la deficiencia de la queja en favor a la peticionaria, en términos del numeral 79 de la Ley de Amparo, **pues el asunto deriva de un juicio oral mercantil en el cual rige el estricto derecho**, sin advertirse además siquiera una violación manifiesta de la ley, por la cual, debe entenderse aquélla visible "*a los ojos del juzgador de manera clara, patente y notoria porque resulta obvia, innegable e indiscutible, sin que para decidir al respecto sea necesario realizar una serie de razonamientos,*

investigaciones y planteamientos cuestionables",[57] lo cual, no ocurre en la especie, pues no salta a la vista alguna inexactitud patente en el actuar de la juez responsable, se concluye que la inconforme no demostró la transgresión de los principios, preceptos y derechos fundamentales mencionados en su demanda y, por ende, debe ***negarse la protección constitucional***.

Cabe indicar que, la negativa del amparo, se **hace extensiva a los actos de ejecución atribuidos al Secretario ejecutor, por no haberse reclamado por vicios propios**.

Apoya lo considerado, la tesis del Quinto Tribunal Colegiado en Materia de Trabajo del Primer Circuito, la cual se comparte, y cuyo contenido es el siguiente:[58]

> ***"AUTORIDADES EJECUTORAS, EXTENSIÓN DE LOS EFECTOS DEL AMPARO NEGADO RESPECTO DE LA ORDENADORA.*** *Si el amparo se niega respecto de la autoridad ordenadora, igual resolución debe emitirse respecto de las ejecutoras, en acatamiento, a contrario sensu, de la jurisprudencia número 70 del Tomo Común al Pleno y a las Salas, del Apéndice de Jurisprudencia de los años 1917-1985, con el rubro: "autoridades ejecutoras, actos de, no reclamados por vicios propios".*

DÉCIMO. Amparo adhesivo. En relación con la demanda de amparo adhesivo presentada por la tercera interesada ***** ******* ******** ******* ** *******

[57] Así lo refirió la Primera Sala de la Suprema Corte de Justicia de la Nación, al resolver el amparo directo en revisión 782/2007.
[58] Localizable en el Semanario Judicial de la Federación, Octava Época, Tomo V, Segunda Parte-1, enero-junio de 1990, página 113, registro 225505.

********, debe indicarse que **por regla general, cuando se niega la protección constitucional en el principal, debe declararse sin materia el adhesivo**.

Sin embargo, dado que en el presente asunto la adherente, dentro de sus conceptos de violación adhesivos, hizo valer una causal de improcedencia del amparo principal, la cual previamente fue desestimada, fue necesario realizar un pronunciamiento respecto de sus motivos de disenso, lo cual, impide declarar sin materia el amparo adhesivo, porque sí la hubo para pronunciarse respecto a un aspecto de procedencia planteado, aunque haya resultado *infundado*.

En consecuencia, los restantes conceptos de violación adhesivos que, en cierto modo, se encaminan a tratar de desvirtuar los principales, deben declararse ***inoperantes***, pues más allá de su impertinencia técnica por atacar los conceptos de violación principales y no reforzar propiamente las consideraciones de la sentencia reclamada ni controvertir un punto decisorio susceptible de perjudicar, lo cierto es que el acto reclamado ha quedado firme, lo cual, era el propósito de la adherente; de ahí el resultar ocioso hacer mayor pronunciamiento al respecto y, ante la inoperancia de los conceptos de violación adhesivos, debe **negarse el amparo a la adherente**.

Sirve de apoyo a lo anterior, por analogía, la jurisprudencia **P./J. 11/2015 (10a.)**,[59] sustentada por el Pleno de la Suprema Corte de Justicia de la Nación, cuyo contenido es:

[59] Publicada en la Gaceta del Semanario Judicial de la Federación, Décima Época, Libro 18, mayo de 2015, Tomo I, página 31, registro 2009170.

“AMPARO ADHESIVO. EL TRIBUNAL COLEGIADO DE CIRCUITO DEBE ESTUDIAR TANTO LA PROCEDENCIA COMO LOS PRESUPUESTOS DE LA PRETENSIÓN, PARA DETERMINAR SI ES FACTIBLE SOBRESEER EN ÉL, DEJARLO SIN MATERIA, NEGARLO O CONCEDERLO. *El artículo 182 de la Ley de Amparo distingue entre los requisitos de procedencia del amparo adhesivo y los presupuestos de la pretensión, por lo que en un primer momento, el Tribunal Colegiado de Circuito debe verificar la procedencia del amparo adhesivo y si alguna de las cuestiones de procedencia previstas en el artículo referido no se actualiza, deberá sobreseer en el juicio de amparo adhesivo, al actualizarse una causal de improcedencia, de conformidad con el artículo 61, fracción XXIII, en relación con el 182, ambos de la Ley de Amparo. En un segundo momento, de resultar procedente el amparo adhesivo, el órgano colegiado, en respeto al principio de exhaustividad, debe analizar de manera conjunta lo planteado tanto en el amparo principal, como en el adhesivo y, de acuerdo con ello, determinar si existe algún argumento planteado en éste al que deba dar respuesta de forma específica -como puede ser alguno respecto a la improcedencia del amparo principal o el análisis de una violación procesal de forma conjunta con algún argumento hecho valer en el amparo principal-, supuesto en el cual el órgano colegiado deberá avocarse a su estudio y realizar las calificativas correspondientes. En otro aspecto, en los casos en que no prospere el amparo principal, sea por cuestiones procesales o por desestimarse los conceptos de violación formulados en la demanda de amparo y sea innecesario realizar un pronunciamiento específico respecto de lo planteado en el amparo adhesivo, resultará necesario declarar éste sin materia. Por otro lado, si los conceptos de violación en el amparo principal se consideran fundados, el Tribunal Colegiado de Circuito debe avocarse al conocimiento de la argumentación del quejoso adherente, cuando ésta pretende abundar en las consideraciones de la sentencia, laudo o resolución reclamada, reforzando los fundamentos de derecho y motivos fácticos de los cuales se valió el órgano jurisdiccional responsable para darle la razón, así como de la violación en el dictado de la sentencia que pudiera afectarle, por*

haberse declarado fundado algún concepto de violación en el amparo principal. Consecuentemente, el órgano colegiado debe atender tanto a los requisitos de procedencia, como a los presupuestos de la pretensión para considerar improcedente el amparo adhesivo y sobreseer en él, declararlo sin materia o calificar los conceptos de violación para negar o conceder el amparo, según corresponda".

Lo anterior, sin perjuicio de que la demanda de amparo adhesivo, en un primer momento, se haya dirigido al juicio de amparo directo ********, y que en dicho precedente, el entonces Magistrado Presidente, mediante auto de veintiséis de noviembre de dos mil veinte,[60] al remitirla a la juez responsable para su tramitación haya considerado que se trataba de un amparo *"principal"*; lo anterior, pues la realidad es que de su parte expositiva y texto, incluyendo sus puntos petitorios, se advierte expresamente que la tercera interesada ***** ******* ******** ******* ** ******* ** ******, indicó que se trata de un amparo adhesivo al principal en donde se reclamó la sentencia combatida de ocho de octubre de dos mil veinte, promovido por ***** ******** ** ******* ******** ******** ********** *** ***** ********** *******, radicada en este expediente 20/2021;

de ahí que correctamente en proveído de Presidencia de veinticuatro de febrero de dos mil veintiuno,[61] se haya dado correctamente el trámite de adhesivo, más allá de lo indicado en el primer auto mencionado pues ello no constituyó una radicación.

Lo anterior sin perjuicio que, de cualquier manera, los autos de presidencia no causan estado, porque en todo caso

[60] Foja 426; *del juicio oral mercantil 96/2018.*
[61] Fojas 71 a 78; *del cuaderno de amparo.*

constituyen resoluciones no definitivas sujetas a lo decidido por este Pleno como potestad de cierre del derecho tal aspecto.

Se invoca en apoyo, por analogía, la jurisprudencia **P./J. 19/98**,[62] sustentada por el Pleno de la Suprema Corte de Justicia de la Nación, del contenido siguiente:

> ***"REVISIÓN EN AMPARO. NO ES OBSTÁCULO PARA EL DESECHAMIENTO DE ESE RECURSO, SU ADMISIÓN POR EL PRESIDENTE DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN.*** *La admisión del recurso de revisión por el presidente de la Suprema Corte de Justicia de la Nación constituye una resolución que no es definitiva, ya que el Tribunal Pleno está facultado, en la esfera de su competencia, para realizar el estudio a fin de determinar la procedencia del recurso y, en su caso, resolver su desechamiento".*

Decisión.

Con base en lo razonado en esta ejecutoria, lo procedente es **negar la protección constitucional tanto en el amparo principal como en el adhesivo.**

Por lo expuesto y fundado se resuelve:

PRIMERO. La Justicia de la Unión **no ampara ni protege** a ***** ******** ** ******* ******** ********* ********** *** ***** ********** *******, en el principal, contra el acto reclamado a la entonces **Juez Séptimo Especializado en Materia Oral Mercantil del Primer Partido Judicial del Estado de Jalisco**, actualmente denominada **Juez Décimo Séptimo en Materia Mercantil**

[62] Publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo VII, marzo de 1998, página 19, registro 196731.

LA PRESENTE FOJA CORRESPONDE A LA PARTE FINAL DE LA SENTENCIA EMITIDA EN SESIÓN VIRTUAL DE **VEINTITRÉS DE SEPTIEMBRE DE DOS MIL VEINTIUNO,** EN EL AMPARO DIRECTO **20/2021,** EL CUAL NEGÓ EL AMPARO PRINCIPAL SOLICITADO Y NEGÓ EL AMPARO ADHESIVO SOLICITADO. CONSTE.-

de la misma circunscripción, consistente en la sentencia definitiva de **ocho de octubre de dos mil veinte**, emitida en el juicio oral mercantil *******, y su ejecución, atribuida al **secretario adscrito a tal órgano jurisdiccional**.

SEGUNDO. La Justicia de la Unión **no ampara ni protege** a ***** ******* ******** ******* ** ******* ********, en el juicio de amparo adhesivo al señalado en el resolutivo previo.

Notifíquese, háganse las anotaciones pertinentes en el libro de gobierno, con testimonio de esta resolución vuelvan los autos al lugar de su procedencia y, en su oportunidad, archívese el presente expediente.

Así lo resolvió el Segundo Tribunal Colegiado en Materia Civil del Tercer Circuito, por unanimidad de votos de los Magistrados Presidente y Ponente **Alberto Miguel Ruiz Matías**, **Víctor Manuel Flores Jiménez** y **Samuel Alberto Villanueva Orozco**. Firman los integrantes del Pleno de este Tribunal Colegiado, con el Secretario de Acuerdos licenciado **Rafael Adrián Castillo Castro**, quien autoriza y da fe.

Firmados.- El Magistrado Presidente y Ponente Alberto Miguel Ruiz Matías.- El Magistrado Víctor Manuel Flores Jiménez.- El Secretario en Funciones de Magistrado de Circuito Armando Márquez Álvarez.- El Secretario de Acuerdos Licenciado Rafael Adrián Castillo Castro.-

Rúbricas.- Es copia fiel sacada de su original de donde se compulsó en **cuarenta y tres fojas útiles**, para remitirse al **Juez Décimo Séptimo**

en Materia Mercantil del Primer Partido Judicial del Estado de Jalisco, tal y como está ordenando en la parte final de esta ejecutoria.-

Zapopan, Jalisco, veintitrés de septiembre de dos mil veintiuno.

EL SECRETARIO DEL SEGUNDO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL TERCER CIRCUITO.

LICENCIADO SHELIN JOSUÉ RODRÍGUEZ RAMÍREZ.

Evidencia Criptográfica – Transacción

Archivo Firmado: 01280000276119940007007.doc

Autoridad Certificadora: Autoridad Certificadora Intermedia del Consejo de la Judicatura Federal

Firmante(s):

Firmante	**Nombre:**	Shelin Josué Rodríguez Ramírez	**Validez:**	OK	Vigente
Firma	**# Serie:**	706a6620636a660000000000000000000000015cf2	**Revocación**	OK	No Revocado
	Fecha: (UTC / Ciudad de México)	30/09/2021T22:24:40Z / 30/09/2021T17:24:40-05:00	**Status:**	OK	Valida
	Algoritmo:	Sha256withRSA			
	Cadena de Firma:	72 24 e1 cc 6a 7e 8f 15 0c 2a 96 5f a0 ca c5 24 65 83 39 79 64 52 c7 41 91 9e c9 a1 75 12 8f e3 c7 48 23 dd d7 e0 e0 66 ae 7b bc 5c aa fa 62 1e 1e 72 80 67 6b ee 7e 65 b0 86 4b ce 8c 3f 97 e4 a8 16 c3 30 c5 8b 0a 2a b4 3b a6 2f a8 36 d2 30 0b 33 a7 d4 22 3c a5 f3 45 59 2c 7a 8f 5b 17 56 5c 33 4e d6 ec 50 b8 8d db f0 cb 0d b5 19 85 84 c7 25 88 31 2f 9c a3 77 ab b8 cf 61 ca 09 fd 6c 74 e9 e6 ef 0d 43 56 7c af 43 bf fd 4f d2 83 60 74 e1 53 4b cf 9f 39 19 83 d8 04 ee 22 aa 64 a9 ad 57 35 c5 3f 23 56 7b 56 78 99 e5 1e 55 08 87 f8 8c e4 d7 43 08 15 d3 2f b0 1e f6 7b 7c 79 88 e6 ec d0 a8 47 f7 5b 24 d3 d2 88 7d 34 cd aa 4e 2a 95 31 08 5b 88 06 3c a8 40 bd 9a ff c2 af ad bb 26 1e c4 44 db 38 64 36 85 71 8b 7e a8 92 98 17 ef 72 9f d5 b8 95 8d 35 bf 4e 84 1e 26 f9 a9			
OCSP	**Fecha: (UTC / Ciudad de México)**	30/09/2021T22:24:40Z / 30/09/2021T17:24:40-05:00			
	Nombre del respondedor:	OCSP ACI del Consejo de la Judicatura Federal			
	Emisor del respondedor:	Autoridad Certificadora Intermedia del Consejo de la Judicatura Federal			
	Número de serie:	70.6a.66.20.63.6a.66.03			

El treinta de septiembre de dos mil veintiuno, el licenciado Shelin Josué Rodríguez Ramírez, Secretario(a), con adscripción en el Segundo Tribunal Colegiado en Materia Civil del Tercer Circuito, hago constar y certifico que en términos de lo previsto en los artículos 108 y 113 fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, esta versión pública suprime toda aquella información considerada legalmente como CONFIDENCIAL, por tratarse de Contiene datos de personas identificadas o identificables.. Conste.