

AMPARO EN REVISIÓN 74/2024

QUEJOSA Y RECURRENTE: *****

RECURRENTE ADHESIVO: SECRETARIO DE
HACIENDA Y CRÉDITO PÚBLICO

PONENTE: MINISTRA LENIA BATRES GUADARRAMA

SECRETARIO: ANGEL JONATHAN GARCÍA ROMO
COLABORÓ: JUAN MACÍAS CRUZ

SÍNTESIS

Hechos: Una persona solicitó a la institución bancaria con la que tiene aperturada una cuenta, el acceso y cancelación de los datos de localización geográfica en tiempo real de los dispositivos en los que realizó operaciones en la banca electrónica. En respuesta, el banco le informó los datos asociados a su persona y, en cuanto a la cancelación, le indicó que era improcedente pues al ser cliente activa sus datos personales eran necesarios para la operación de los productos y servicios contratados.

Inconforme, la titular de datos personales acudió al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) para solicitar la protección de sus datos personales. Durante la tramitación del procedimiento, la institución bancaria modificó su respuesta, dio acceso a la titular a sus datos de geolocalización y declaró procedente la cancelación. Le informó que debía transcurrir el período de bloqueo correspondiente al plazo de prescripción legal y después procedería su supresión. Seguido el procedimiento, el INAI dictó resolución y confirmó la respuesta del banco, dio acceso a la titular a los datos personales y accedió a la cancelación, previo transcurso del período de bloqueo, tras el cual se haría la supresión.

En desacuerdo, la titular de datos personales promovió amparo contra ciertas normas contenidas en la Resolución que reforma, adiciona y deroga diversas de las Disposiciones de Carácter General a que se refiere el artículo 115 de la Ley de Instituciones de Crédito (LIC), publicada en el Diario Oficial de la Federación (DOF) el veintidós de marzo de dos mil diecinueve, con motivo de su aplicación. Previa tramitación correspondiente, el juez de distrito, por una parte, sobreseyó en el juicio por cesación de efectos de la geolocalización reclamada del banco, decisión que hizo extensiva a las normas controvertidas y, por otra, negó el amparo contra la resolución.

Inconforme, la quejosa interpuso recurso de revisión al que se adhirió el Secretario de Hacienda y Crédito Público. Substanciado el procedimiento, el tribunal colegiado de circuito del conocimiento dictó resolución, modificó el sobreseimiento decretado en el juicio de amparo. Sobreseyó por cambio de situación jurídica respecto del acto de aplicación reclamado del banco consistente en la respuesta a la solicitud de acceso y cancelación de datos personales y su modificación, ya que esas determinaciones fueron sustituidas por la resolución del órgano garante que puso fin al procedimiento de solicitud de protección de datos personales. Determinó que la resolución es el acto concreto de aplicación de las normas reclamadas y,

AMPARO EN REVISIÓN 74/2024

finalmente, solicitó a esta Suprema Corte de Justicia de la Nación (SCJN) reasumiera su competencia originaria para conocer del tema de constitucionalidad de normas subsistente.

ÍNDICE TEMÁTICO

	Apartado	Criterio y decisión	Págs.
I.	COMPETENCIA	Esta Segunda Sala es competente para conocer del presente asunto.	3-4
II.	OPORTUNIDAD Y LEGITIMACIÓN	Los recursos son oportunos y fueron interpuestos por partes legitimadas.	4
III.	PROCEDENCIA	El asunto reúne los requisitos de procedencia.	4
IV.	CORRECCIÓN DE INCONGRUENCIAS	A. Precisión de actos reclamados. B. Existencia de nuevos actos reclamados. C. Análisis de causas de improcedencia pendientes de estudio. Una es fundada y las demás infundadas.	4-10
V.	ESTUDIO DE FONDO V.1. PLAZO DE BLOQUEO DE DATOS PERSONALES	Son infundados los argumentos de la quejosa, pues la existencia del plazo de bloqueo y su duración están justificados.	10 a 13
	V.2. GEOLOCALIZACIÓN DE DISPOSITIVOS CON ACCESO A INTERNET	Son infundados los argumentos de la quejosa.	13 a 30
VI.	REVISIÓN ADHESIVA	Sin materia.	30
VII.	DECISIÓN	PRIMERO. En la materia del recurso, se MODIFICA la sentencia recurrida. SEGUNDO. Se SOBRESEE en el juicio respecto de la disposición tercera transitoria, fracción V, de la Resolución que reforma, adiciona y deroga diversas de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito, publicada en el Diario Oficial de la Federación el veintidós de marzo del dos mil diecinueve. TERCERO. La Justicia de la Unión NO AMPARA NI PROTEGE a ***** ***** contra los artículos 25 de la Ley Federal de Protección de Datos Personales en Posesión de	30-31

AMPARO EN REVISIÓN 74/2024

		<p>los Particulares, 105 y 107 de su reglamento y las disposiciones 4 Ter, primer párrafo y fracción VII, 16 Bis, párrafos segundo y tercero, 24, párrafo segundo, 25 Bis, párrafo cuarto, de la Resolución que reforma, adiciona y deroga diversas de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito, publicada en el Diario Oficial de la Federación el veintidós de marzo del dos mil diecinueve, en materia de geolocalización, así como contra la resolución de veintidós de febrero del dos mil veintitrés dictada por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el expediente *****.</p> <p>CUARTO. Queda SIN MATERIA la revisión adhesiva.</p>	
--	--	--	--

AMPARO EN REVISIÓN 74/2024

QUEJOSA Y RECURRENTE: *****

RECURRENTE ADHESIVO: SECRETARIO DE HACIENDA Y CRÉDITO PÚBLICO

VISTO BUENO
SRA. MINISTRA

PONENTE: LENIA BATRES GUADARRAMA

COTEJÓ

**SECRETARIO: ANGEL JONATHAN GARCÍA ROMO
COLABORÓ: JUAN MACÍAS CRUZ**

Ciudad de México. Esta Segunda Sala de la Suprema Corte de Justicia de la Nación (SCJN) correspondiente al

***** de ** del dos mil veinticuatro, emite la siguiente:

SENTENCIA

Mediante la cual se resuelve el recurso de revisión 74/2024, interpuesto contra la sentencia dictada el veintiuno de agosto del dos mil veintitrés por el Juez Décimo Quinto de Distrito en Materia Administrativa de la Ciudad de México, en el juicio de amparo indirecto *****.

El problema jurídico por resolver en esta Segunda Sala de la SCJN consiste en determinar la constitucionalidad o no de las normas reclamadas contenidas en la Resolución que reforma, adiciona y deroga diversas de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito, publicada en el DOF el veintidós de marzo del dos mil diecinueve.

ANTECEDENTES Y TRÁMITE

1. **Solicitud de derechos ARCO.** El veinte de julio de dos mil veintidós, la quejosa, cliente de BBVA México, Sociedad Anónima, Institución de Banca Múltiple, Grupo Financiero BBVA México, solicitó el acceso y cancelación de los datos de localización geográfica en tiempo real de los dispositivos a través de los que realizó operaciones de banca electrónica. En respuesta, el banco le informó los datos asociados a su persona y, en cuanto a la cancelación, le indicó que era improcedente, pues al ser cliente activa sus datos personales eran necesarios para la operación de los productos y servicios contratados.
2. **Solicitud de protección de derechos.** En desacuerdo, la titular de datos personales solicitó al INAI la protección de derechos, que fue registrada con el expediente *****.
3. **Modificación de la respuesta.** Durante la sustanciación del procedimiento, la institución bancaria modificó su respuesta en los términos siguientes:
 - a. Respecto a la solicitud de acceso, acompañó documentos en los que constan los registros de geolocalización de las operaciones de canales remotos llevadas a

cabo por la titular de la cuenta, durante el periodo comprendido entre el momento en que entró en vigor la obligación de obtención de dichos datos y aquel en que fue notificada la solicitud de protección de datos.

- b. En relación con la solicitud de cancelación, modificó su respuesta e indicó que resultó procedente con el correspondiente periodo de bloqueo en el que la institución bancaria conserva y utiliza los datos de geolocalización exclusivamente para efectos del cumplimiento de las responsabilidades derivadas de las disposiciones de carácter general a que se refiere el artículo 115 de la LIC, principalmente la disposición 59ª, por lo que, el periodo de bloqueo sería equivalente al plazo de conservación y prescripción legal establecido en dicha norma, tras el cual se procedería a su supresión.

4. **Resolución administrativa.** El veintidós de febrero del dos mil veintitrés, el Pleno del INAI resolvió confirmar la respuesta de la institución bancaria, pues consideró que, respecto al derecho de acceso, durante el procedimiento se entregó a la quejosa los datos de geolocalización tanto en físico como en formato digital y, por lo que hace al derecho de cancelación, estimó apegada a derecho la determinación del banco en el sentido de que procedía tras el periodo de bloqueo aplicable.

5. **Demanda de amparo.** Por escrito recibido el treinta y uno de marzo de dos mil veintitrés en el Portal de Servicios en Línea del Poder Judicial de la Federación (PJF), la titular de datos personales, por propio derecho, promovió juicio de amparo contra el Secretario de Hacienda y Crédito Público, el Pleno del INAI y BBVA México, Sociedad Anónima, Institución de Banca Múltiple, Grupo Financiero BBVA México, de quienes reclamó en el respectivo ámbito de sus competencias o atribuciones lo siguiente:

- a. Los numerales 4ª Ter, primer párrafo y fracción VII, 16ª Bis, párrafos segundo y tercero, 24ª, párrafo segundo, 25ª bis, párrafo cuarto y la disposición Transitoria Tercera, fracción V, de la Resolución que reforma, adiciona y deroga diversas de las disposiciones de carácter general a que se refiere el artículo 115 de la LIC, publicada en el DOF el veintidós de marzo del dos mil diecinueve.

- b. La indebida interpretación de las obligaciones contenidas en tales disposiciones, materializada en la resolución de veintidós de febrero del dos mil veintitrés dictada en el expediente *****.

- c. La aplicación de tales disposiciones y que se traducen en la recolección, almacenamiento prolongado y la transferencia automática de los datos de localización geográfica.

6. **Sentencia de amparo.** Seguido el trámite del juicio de amparo ***** , el Juez Décimo Quinto de Distrito en Materia Administrativa en la Ciudad de México (CDMX) dictó sentencia el veintiuno de agosto del dos mil veintitrés, en la que **sobreseyó** en el juicio por la negativa a la solicitud de cancelación de datos personales por haber cesado sus efectos, decisión que hizo extensiva a las disposiciones generales reclamadas; desestimó la causa de improcedencia que hizo valer el INAI consistente en la falta de interés jurídico y, finalmente, **negó el amparo** contra la resolución emitida por el Pleno del INAI al considerar inoperantes los conceptos de violación.

7. **Recurso de revisión.** Contra la sentencia, la quejosa interpuso recurso de revisión, del cual conoció Primer Tribunal Colegiado en Materia Administrativa del Primer Circuito, quien lo registró como expediente ***** , al que se adhirió la SHCP.

8. **Resolución.** El veinticinco de enero de dos mil veinticuatro, el tribunal emitió resolución en la que modificó el sobreseimiento. Sobreseyó por cambio de situación

jurídica por el acto de aplicación reclamado del banco consistente en la respuesta a la solicitud de acceso y cancelación de datos personales y su modificación, ya que esas determinaciones fueron sustituidas por la resolución del órgano garante que puso fin al procedimiento de solicitud de protección de datos personales. Determinó que la resolución es acto concreto de aplicación de las normas reclamadas y, finalmente, solicitó a esta SCJN reasumiera su competencia originaria para conocer del tema de constitucionalidad de normas subsistente.

9. **Trámite ante la SCJN.** En auto de ocho de febrero del dos mil veinticuatro, la Presidenta asumió la competencia originaria de esta SCJN para conocer del recurso de revisión y su adhesión, se registró con el expediente **74/2024**, ordenó su turno al Ministro Javier Laynez Potisek y remitió los autos a esta Segunda Sala a la que se encuentra adscrito.
10. **Avocamiento.** Mediante acuerdo de uno de marzo siguiente, esta Segunda Sala se avocó al conocimiento del asunto remitiendo los autos al ministro ponente.
11. **Retorno.** En sesión de veintisiete de noviembre de dos mil veinticuatro, por mayoría de tres votos se desechó el proyecto de resolución presentado por el Ministro Javier Laynez Potisek, razón por la que se retornó el asunto a la Ministra Lenia Batres Guadarrama.¹
12. **Publicación del proyecto.** El proyecto de sentencia fue publicado de conformidad con lo dispuesto por los artículos 73, párrafo segundo, y 184, párrafo primero, de la Ley de Amparo.

I.COMPETENCIA

13. Esta Segunda Sala de la SCJN es competente para conocer del presente amparo en revisión en términos de lo dispuesto en los artículos 107, fracción VIII, inciso a, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM),² 81, fracción I, inciso e, de la Ley de Amparo;³ 10, fracción III, de la Ley Orgánica del Poder Judicial de la Federación (LOPJF);⁴ así como en los puntos Segundo, fracción III, inciso A), y Quinto, fracción I, inciso B, interpretado *contrario sensu*, del Acuerdo General Plenario 1/2023,⁵ publicado en el DOF el tres de febrero de dos mil

¹ Acuerdo de dos de diciembre del dos mil veinticuatro.

² **Art. 107.-** Las controversias de que habla el artículo 103 de esta Constitución, con excepción de aquellas en materia electoral, se sujetarán a los procedimientos que determine la ley reglamentaria, de acuerdo con las bases siguientes:

VIII.- Contra las sentencias que pronuncien en amparo las Juezas y los Jueces de Distrito o los Tribunales Colegiados de Apelación procede revisión. De ella conocerá la Suprema Corte de Justicia:

a) Cuando habiéndose impugnado en la demanda de amparo normas generales por estimarlas directamente violatorias de esta Constitución, subsista en el recurso el problema de constitucionalidad.

³ **Artículo 81.** Procede el recurso de revisión:

I. En amparo indirecto, en contra de las resoluciones siguientes:

e) Las sentencias dictadas en la audiencia constitucional; en su caso, deberán impugnarse los acuerdos pronunciados en la propia audiencia.

⁴ **Artículo 10.** La Suprema Corte de Justicia de la Nación conocerá funcionando en Pleno:

III. Del recurso de revisión contra sentencias pronunciadas en la audiencia constitucional por los juzgados de distrito o los tribunales colegiados de apelación, cuando habiéndose impugnado en la demanda de amparo normas generales por estimarlas directamente violatorias de la Constitución Política de los Estados Unidos Mexicanos, subsista en el recurso el problema de constitucionalidad;

⁵ **SEGUNDO.** El Tribunal Pleno de la Suprema Corte de Justicia de la Nación conservará para su resolución:

III. Los amparo en revisión:

A) Tramitados en la vía indirecta, en los que, subsistiendo la materia de constitucionalidad de leyes federales o tratados internacionales, no exista precedente y, a su juicio, se requiera fijar un criterio de importancia y trascendencia para el orden jurídico nacional;

(...)

QUINTO. De los asuntos de la competencia originaria de la Suprema Corte de Justicia de la Nación, corresponderá resolver a los Tribunales Colegiados de Circuito:

veintitrés, porque se interpuso contra una sentencia dictada por el juez de distrito, en que subsiste el problema de constitucionalidad de normas, sin que se estime necesaria la intervención del Tribunal Pleno.

II. OPORTUNIDAD Y LEGITIMACIÓN

14. Es innecesario el estudio de la oportunidad de los recursos principal y adhesivo porque dicho presupuesto procesal fue analizado por el tribunal colegiado del conocimiento.⁶
15. Por otra parte, esta Segunda Sala considera que el recurso de revisión se interpuso por parte legítima pues lo intenta ***** , autorizado de la parte quejosa en el juicio de amparo indirecto de origen en términos amplios, personería que reconoció el juez de distrito mediante acuerdo de tres de abril del dos mil veintitrés.
16. Asimismo, el recurso de revisión adhesivo fue interpuesto por parte legítima pues lo intenta el Director General de Amparos contra Leyes, en suplencia por ausencia de la Subprocuradora Fiscal Federal de Amparos, en representación de la SHCP, autoridad responsable en el juicio de amparo indirecto de origen. Lo anterior de conformidad con lo previsto en el artículo 9o., segundo párrafo, de la Ley de Amparo,⁷ así como en los diversos 28, fracción VII,⁸ en relación con el 4, primer párrafo, Apartado D, fracción II,⁹ del Reglamento Interior de la SHCP.

III. PROCEDENCIA

17. Esta Segunda Sala de la SCJN considera que el asunto reúne los requisitos de procedencia y, por tanto, amerita un estudio de fondo, porque se interpone contra una sentencia dictada por un juez de distrito, en el cual subsiste el tema de constitucionalidad de disposiciones de carácter general cuyo estudio puede implicar el alcance de un derecho humano.

IV. CORRECCIÓN DE INCONGRUENCIAS

I. Los recursos de revisión en contra de sentencias pronunciadas por los Juzgados de Distrito o por los Tribunales Colegiados de Apelación, cuando: (...)

B) En la demanda se hubiere impugnado una ley local, un reglamento federal o local, o cualquier disposición de observancia general, salvo aquéllos en los que el análisis de constitucionalidad respectivo implique fijar el alcance de un derecho humano previsto en tratados internacionales de los que el Estado Mexicano sea parte, respecto del cual no exista jurisprudencia del Pleno o de las Salas de este Alto Tribunal, sin menoscabo de que la Sala en la que se radique el recurso respectivo determine que su resolución corresponde a un Tribunal Colegiado de Circuito; (...)

⁶ Folio 85 y reverso del amparo en revisión 454/2023.

⁷ Artículo 9o.

(...)

El Presidente de la República será representado en los términos que se señalen en el acuerdo general que expida y se publique en el Diario Oficial de la Federación. Dicha representación podrá recaer en el propio Consejero Jurídico o en los secretarios de estado a quienes en cada caso corresponda el asunto, en términos de las leyes orgánicas y reglamentos aplicables. Los reglamentos interiores correspondientes señalarán las unidades administrativas en las que recaerá la citada representación. En el citado acuerdo general se señalará el mecanismo necesario para determinar la representación en los casos no previstos por los mismos.

(...)

⁸ Artículo 28.- La Subprocuraduría Fiscal Federal de Amparos tiene las atribuciones siguientes:

(...)

VII. Representar el interés de la Federación en controversias fiscales; a la Secretaría y a las autoridades dependientes de la misma en toda clase de juicios, investigaciones o procedimientos ante los tribunales de la República, ante la Comisión Nacional de los Derechos Humanos, y ante otras autoridades competentes, en que sean parte, o cuando sin ser parte, sea requerida su intervención por la autoridad que conoce del juicio o procedimiento, o tenga interés para intervenir conforme a sus atribuciones; y, en su caso, poner en conocimiento del Órgano Interno de Control en la Secretaría, los hechos respectivos; ejercitar los derechos, acciones, excepciones y defensas de las que sean titulares, desistimientos y demás promociones que correspondan; transigir cuando así convenga a los intereses de la Secretaría, e interponer los recursos que procedan ante los citados tribunales y autoridades, siempre que dicha representación no corresponda a otra unidad administrativa de la propia Secretaría o al Ministerio Público Federal y, en su caso, proporcionarle los elementos que sean necesarios;

⁹ Artículo 4.- La Secretaría, para el despacho de los asuntos de su competencia, contará con las unidades administrativas y órganos administrativos desconcentrados siguientes:

(...)

D. Procuraduría Fiscal de la Federación:

(...)

II. Subprocuraduría Fiscal Federal de Amparos:

(...)

18. En términos del artículo 76 de la Ley de Amparo¹⁰ y tomando en cuenta que la congruencia de las sentencias que se dicten en los juicios de amparo es una cuestión de orden público, a continuación, se corrigen las incongruencias de las sentencias emitidas por los órganos jurisdiccionales que precedieron en el conocimiento del asunto, amén que en sus agravios la quejosa controvierte la correcta apreciación de los actos reclamados.

A. Precisión actos reclamados:

19. En su demanda de amparo, la quejosa señaló como actos reclamados de manera destacada los siguientes:
- a) Las disposiciones 4 Ter, primer párrafo y fracción VII, 16 Bis, párrafos segundo y tercero, 24, párrafo segundo, 25 Bis, párrafo cuarto y tercera transitoria fracción V, de la Resolución que reforma, adiciona y deroga diversas de las Disposiciones de carácter general a que se refiere el artículo 115 de la LIC, publicada en el DOF el veintidós de marzo del dos mil diecinueve, que reclamó de la SHCP.
 - b) La indebida interpretación de las obligaciones contenidas en dichas disposiciones y que se materializó en la resolución de veintidós de febrero del dos mil veintitrés, dictada por el Pleno del INAI en el procedimiento de protección de derechos *********, que reclamó del citado órgano garante; y
 - c) Los actos de aplicación consistentes en la recolección, almacenamiento prolongado y transferencia automática de los datos de localización geográfica, así como la restricción al derecho de autodeterminación informativa en relación con los derechos de oposición y cancelación de datos personales materializado en la negativa a su solicitud de cancelación de datos personales.
20. En la sentencia recurrida, el juez tuvo como actos reclamados la emisión de las normas antes precisadas, su aplicación a través de la negativa a la solicitud de cancelación de datos personales y la resolución del INAI; sin embargo, no dijo nada en cuanto a los actos reclamados de manera destacada consistentes en la indebida interpretación de las normas reclamadas y la recolección, almacenamiento prolongado, transferencia automática de los datos de localización geográfica y restricción al derecho de autodeterminación informativa.
21. Debe decirse que, si bien la quejosa los señaló como actos reclamados de manera destacada, no deben tenerse como tales por dos razones. La primera, porque en el juicio de amparo la determinación y existencia de los actos reclamados debe realizarse sin tomar en cuenta los calificativos que en su enunciación se hagan sobre su constitucionalidad,¹¹ simple y sencillamente porque constituyen vicios que la parte quejosa atribuye a otros actos reclamados y, la segunda que, de hecho

¹⁰ **Artículo 76.** El órgano jurisdiccional, deberá corregir los errores u omisiones que advierta en la cita de los preceptos constitucionales y legales que se estimen violados, y podrá examinar en su conjunto los conceptos de violación y los agravios, así como los demás razonamientos de las partes, a fin de resolver la cuestión efectivamente planteada, sin cambiar los hechos expuestos en la demanda.

¹¹ Tesis de jurisprudencia de la Segunda Sala, publicada en el Semanario Judicial de la Federación, volumen 18, Tercera Parte, página 159, Séptima Época, registro digital 239099, de rubro: **ACTO RECLAMADO. SU EXISTENCIA DEBE EXAMINARSE SIN TOMAR EN CUENTA LOS CALIFICATIVOS QUE EN SU ENUNCIACION SE HAGAN SOBRE SU CONSTITUCIONALIDAD.**

corroborar lo anterior, porque la solicitante del amparo afirmó que tales vicios se materializaron en ciertos actos concretos como son la respuesta que recibió de la institución bancaria y la resolución del Pleno del INAI que recayó al procedimiento que instó.

22. De ahí que tales actos no deban tenerse como reclamados de manera destacada.
23. Ahora, como se informó en los resultados de esta ejecutoria, el tribunal colegiado de circuito que precedió en el conocimiento del asunto sobreseyó en el juicio por cambio de situación jurídica respecto de las respuestas dadas por la institución bancaria a la solicitud de acceso y cancelación de datos personales formulada por la ahora quejosa, de manera que, a su juicio, sólo subsistían como actos reclamados las normas señaladas de manera destacada por la promovente con motivo de su aplicación efectuada en la resolución del INAI.
24. Al respecto se precisa que, si bien en la resolución el órgano garante no citó expresamente las disposiciones emitidas por la SHCP, es innegable que implícitamente las consideró para confirmar la resolución de la institución bancaria, también es indiscutible que con base en ellas se geolocalizó a la quejosa por las operaciones bancarias que realizó a través de dispositivos de forma no presencial desde el inicio de su vigencia y hasta que modificó la mencionada respuesta.
25. Es más, el hecho de que el banco haya accedido a la cancelación en el tratamiento de datos personales de la quejosa y se haya iniciado el período de bloqueo cuya constitucionalidad también se cuestiona, deja ver que hubo aplicación de las normas que prevén el deber de geolocalización, lo que evidentemente permite a este órgano judicial pronunciarse sobre su constitucionalidad.
26. Finalmente, no debe perderse de vista que si se sobreseyera en el juicio por las disposiciones de carácter general tildadas de inconstitucionales por cesación de efectos como hizo el juez, o bien, por cambio de situación jurídica al existir una resolución posterior del Pleno del INAI, lo cierto es que la quejosa no podría, o bien sería complicado, que en algún momento pudieran controvertir su contenido.
27. Lo anterior, porque bastaría que las instituciones de crédito modificaran una primera respuesta, como ocurrió, para impedir el análisis de constitucionalidad propuesto, haciendo imposible su reclamo. De ahí que proceda el estudio de constitucionalidad del acto concreto de aplicación indicado por el tribunal colegiado.
28. Por tanto, los actos reclamados que subsisten en este asunto son los artículos 25 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y 105 y 107 de su reglamento; las disposiciones 4 Ter, primer párrafo y fracción VII, 16 Bis, párrafos segundo y tercero, 24, párrafo segundo, 25 Bis, párrafo cuarto, y tercera transitoria, fracción V, de la Resolución que reforma, adiciona y deroga diversas de las disposiciones de carácter general a que se refiere el artículo 115 de la LIC, publicada en el DOF el veintidós de marzo del dos mil diecinueve y la resolución de veintidós de febrero del dos mil veintitrés dictada por el Pleno del INAI en el expediente *****.

B. Existencia de nuevos actos reclamados:

29. Constituye un hecho notorio para este órgano colegiado la existencia de la discusión, aprobación, expedición y promulgación del artículo 25 de la LFPDPPP,

así como de la expedición y promulgación de los diversos 105 y 107 de su reglamento.

30. Apoya esta determinación la tesis de jurisprudencia 2a./J. 65/2000 de esta Segunda Sala de la SCJN, de rubro: **PRUEBA. CARGA DE LA MISMA RESPECTO DE LEYES, REGLAMENTOS, DECRETOS Y ACUERDOS DE INTERÉS GENERAL PUBLICADOS EN EL DIARIO OFICIAL DE LA FEDERACIÓN.**¹²

C. Causas de improcedencia pendientes de estudio

31. No obstante, que el tribunal colegiado modificó la decisión del juez de sobreseer en el juicio respecto de las disposiciones de carácter general reclamadas, quedaron pendientes de examen las causas de improcedencia que propuso la autoridad emisora, esto es, la SHCP, razón por la que a continuación se resolverán.
32. La responsable en su informe justificado afirma que en el caso se actualizan las causas de improcedencia previstas en el artículo 61, fracciones XII, XVIII y XX, de la Ley de Amparo, pues a su juicio la quejosa no acreditó su interés jurídico y no respetó el principio de definitividad.
33. Afirma que la primera hipótesis se actualiza porque la quejosa reclamó las normas en su carácter de heteroaplicativas, lo cierto es que omitió demostrar su acto concreto de aplicación, en específico, que la institución bancaria haya recabado la geolocalización de su dispositivo móvil por haber realizado una operación de forma no presencial, pues dice que para ello se requiere necesariamente su consentimiento previo.
34. Entonces, la autoridad sostiene que para acreditar su interés jurídico no sólo era necesario demostrar tener una cuenta bancaria en la institución, sino que abrió la cuenta o realizó una operación de manera no presencial, siendo la documental idónea para el consentimiento otorgado a la institución bancaria para recabar la geolocalización de los dispositivos móviles relacionados con su cuenta.
35. En cuanto a la aplicación de la disposición 24 reclamada, afirma que el documento idóneo para acreditar su aplicación es el contrato de apertura y, también, el consentimiento otorgado a la entidad financiera para recabar la aludida geolocalización, que tampoco se anexaron como pruebas.
36. Para resolver los argumentos se precisa, en principio, que la quejosa no reclamó las normas en su naturaleza de heteroaplicativas, sino con motivo de su acto de aplicación, lo cual es distinto, pues no debe perderse de vista que, aun tratándose de normas autoaplicativas, pueden reclamarse con motivo de su vigencia, o bien, de su primer acto concreto de aplicación.
37. **Se desestiman los argumentos que expone la autoridad** para demostrar la actualización de la causa de improcedencia de falta de interés jurídico, porque parten de una premisa inexacta consistente en el acto de aplicación del que resultó procedente el amparo.

¹² Tesis de jurisprudencia de la Segunda Sala, publicada en el Semanario Judicial de la Federación y su Gaceta, Tomo XII, agosto de 2000, página 260, registro digital 191452.

38. Los argumentos giran en torno a la idea de que la quejosa reclama de la institución bancaria la geolocalización de que fue objeto, sin embargo, pierde de vista que el amparo resultó procedente contra la resolución del Pleno del INAI que confirmó las diversas resoluciones bancarias que dieron acceso a esos datos de localización geográfica y a la cancelación, originando que las avalara.
39. Ello implica, como se dijo, que las disposiciones reclamadas sobre el deber de las instituciones de crédito de geolocalizar las operaciones realizadas por sus clientes de manera no presencial, fueron aplicadas en su perjuicio, tan es así que en la respuesta a través de la que el banco modificó la primigenia, proporcionó a la titular de datos personales la información relativa a la geolocalización de las operaciones que así realizó durante el tiempo de vigencia y hasta la cancelación que efectuó, de modo que es innegable la aplicación de tales disposiciones en su perjuicio.
40. Esa aplicación tuvo verificativo en la resolución dictada en un procedimiento administrativo que la propia quejosa instó, de manera que es innegable que tiene interés jurídico para acudir al amparo.
41. Sin que sea necesario, como alega la autoridad, que la promovente exhibiera el contrato de apertura de la cuenta bancaria, su consentimiento para el tratamiento y obtención de geolocalización de las operaciones realizadas vía remota, la realización de alguna de ellas, o bien, algún otro documento tendente a demostrar que realizó tales operaciones en virtud de las cuales la institución bancaria la localizó geográficamente, pues para evidenciar la aplicación en su perjuicio basta la resolución recaída al procedimiento de protección de derechos que la quejosa promovió ante el INAI y, eventualmente, la respuesta modificada que emitió la institución bancaria.
42. Respecto de la misma causa de improcedencia, la SHCP afirma que las normas reclamadas no irrogan perjuicio a la promovente porque están dirigidas a las entidades que abran una cuenta o celebren un contrato a través de dispositivos de forma no presencial, no así a los clientes o usuarios.
43. Insiste en que las disposiciones reclamadas están dirigidas a las instituciones de crédito, razón por la que no causan perjuicio en la esfera jurídica de la quejosa, en tanto, sólo establecen un procedimiento posterior a través del que da un tratamiento a los usuarios que no brinden su consentimiento para la geolocalización de sus dispositivos.
44. Dicha causa de improcedencia también debe desestimarse respecto de las disposiciones 4 Ter, primer párrafo y fracción VII, 16 Bis, párrafos segundo y tercero, 24, párrafo segundo, 25 Bis, párrafo cuarto, de la Resolución en comento, en la medida en que aun cuando se acepte que tales disposiciones sólo vinculan a las instituciones de crédito a recabar los datos de geolocalización de los dispositivos utilizados por sus clientes o usuarios cuando realicen operaciones a distancia, es claro que impacta en ellos, porque son las personas que realizan esas operaciones. De ahí que sea infundada la causa de improcedencia analizada.
45. A conclusión, distinta debe arribarse respecto de la disposición tercera transitoria, fracción V, de la Resolución en materia, pues sólo vincula a la institución de crédito a recabar la geolocalización del dispositivo desde el cual el cliente o usuario celebre cada operación no presencial, en el plazo de veinticuatro meses contado a partir de su entrada en vigor, de manera que no irroga perjuicio en la esfera jurídica de la quejosa, amén que ese plazo ya transcurrió.

46. En las relatadas circunstancias, se impone **sobreseer** en el juicio respecto de la disposición tercera transitoria, fracción V, de la Resolución que reforma, adiciona y deroga diversas de las Disposiciones de carácter general a que se refiere el artículo 115 de la LIC, publicada en el mencionado órgano de difusión oficial el veintidós de marzo del dos mil diecinueve, con fundamento en lo dispuesto en los artículos 61, fracción XII, y 63, fracción V, de la Ley de Amparo.
47. Por otra parte, la responsable afirma que el juicio se debe sobreseer al actualizarse las causas de improcedencia contenidas en las fracciones XVIII y XX del artículo 61 de la Ley de Amparo.
48. La primera de tales fracciones establece que el juicio de amparo es improcedente contra las resoluciones de tribunales judiciales, administrativos o del trabajo, respecto de las cuales conceda la ley ordinaria algún recurso o medio de defensa, dentro del procedimiento, por virtud del cual puedan ser modificadas, revocadas o nulificadas.
49. Independientemente de las excepciones que prevé la propia fracción, es claro que la causa de improcedencia no se actualiza porque el acto concreto de aplicación reclamado no fue emitido por tribunales judiciales, administrativos o del trabajo, sino por el órgano garante en materia de transparencia y protección de datos personales.
50. Por su parte, la fracción XX dispone que el amparo es improcedente contra actos de autoridades distintas de los tribunales judiciales, administrativos o del trabajo, que deban ser revisados de oficio, conforme a las leyes que los rijan o proceda contra ellos algún juicio, recurso o medio de defensa legal por virtud del cual puedan ser modificados, revocados o nulificados, siempre que conforme a las mismas leyes se suspendan sus efectos, con los mismos alcances que los que prevé la Ley de Amparo y sin exigir mayores requisitos que los necesarios para conceder la suspensión definitiva, ni plazo mayor que el que establece para el otorgamiento de la suspensión provisional, independientemente de que el acto en sí mismo considerado sea o no susceptible de ser suspendido.
51. Tal disposición prevé la causa de improcedencia relacionada con el principio de definitividad que exige que antes de acudir al amparo la parte quejosa agote los medios ordinarios de defensa, siempre que se actualicen las condiciones que el propio precepto prevé.
52. La autoridad sostiene que la quejosa debió acudir al juicio mercantil antes que, al amparo, pues la geolocalización de la que se duele deriva de un contrato de adhesión que celebró con una institución bancaria, de modo que debió acudir a aquella vía para controvertir la solicitud de geolocalización.
53. Como se ve, el argumento de la autoridad parte de diversas premisas inexactas. La primera consiste en que el juicio de amparo se promovió contra la solicitud de geolocalización, siendo que, como se resolvió, procede contra las normas que prevén dicha geolocalización, con motivo de su aplicación en la resolución emitida por el INAI. Luego, la geolocalización controvertida si bien deriva de un contrato de adhesión, lo objetivamente cierto es que la promovente reclama las disposiciones

que la establecen con motivo de su confirmación por parte del órgano garante en materia de protección de datos personales.

54. Finalmente, porque aun cuando fuera así, la autoridad pierde de vista que una de las excepciones al principio de definitividad es precisamente la impugnación de normas y más, cuando su aplicación pudiere ser de imposible reparación, como en el caso en que la geolocalización afectara derechos sustantivos de la solicitante de amparo.
55. En consecuencia, es **infundada** la causa de improcedencia en estudio.
56. Al no existir alguna otra causa de improcedencia pendiente de estudio, o bien, que este órgano judicial advierta de oficio, se procede al análisis y resolución del fondo del asunto.

V. ESTUDIO DE FONDO

57. En virtud de que el tribunal colegiado levantó el sobreseimiento de las normas reclamadas al considerar que fueron aplicadas implícitamente por el INAI en la resolución que recayó al procedimiento de protección de datos, a continuación, se resolverán los conceptos de violación que la quejosa propone.
58. Por cuestión de método, primero, se resolverá el argumento vinculado con las normas que prevén el plazo de bloqueo de los datos personales una vez efectuada la cancelación del tratamiento. Luego, el tema relacionado con el deber de las instituciones de crédito de obtener la geolocalización de los dispositivos con acceso a internet utilizados por sus clientes o usuarios al realizar operaciones bancarias no presenciales. Finalmente, la posible violación a la garantía de seguridad jurídica en su vertiente de reserva de ley.

V.1. PLAZO DE BLOQUEO DE DATOS PERSONALES

59. En una parte de su segundo concepto de violación, la quejosa afirma que los artículos 25 de la LFPDPPP, 105 y 107 de su reglamento, son inconstitucionales porque prevén el almacenamiento indeterminado y prolongado de sus datos personales.
60. Sustenta su alegato, en que conforme a tales normas las instituciones de crédito se encuentran obligadas a almacenar los datos de geolocalización por un periodo de tiempo “no menor a diez años, contado a partir de la ejecución de la operación realizada por sus clientes o usuarios”; lo que implica que de manera injustificada continuará tratando esa información pese a que el titular solicitó su cancelación.
61. Para resolver su argumento conviene señalar que en el artículo 16, párrafo segundo, de la CPEUM se establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y su cancelación, así como a expresar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
62. Tal disposición reconoce, entre otras cosas, el derecho de protección de datos personales en nuestro país, así como la existencia y salvaguarda de los denominados derechos ARCO que son la posibilidad de que las personas puedan

acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales que realice el sujeto obligado, o bien, el particular, según sea el caso.

63. En el artículo 3o., fracción III, de la LFPDPPP se define al bloqueo como la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas.

64. Se prevé en tal disposición que, durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido ese lapso, se procederá a su cancelación en la base de datos que corresponde.
65. Por su parte, en el artículo 25 reclamado se dispone que el titular de datos personales tiene en todo momento el derecho a cancelar su tratamiento, la cual dará lugar a un periodo de bloqueo tras el que se procederá a la supresión de la información.
66. En la segunda parte del párrafo segundo se dispone que el responsable podrá conservar los datos exclusivamente para efectos de las responsabilidades nacidas del tratamiento y que el periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que justifica el tratamiento en los términos de la ley aplicable en la materia.
67. Conforme al resto de la norma en comento, una vez cancelado el dato se avisará a su titular y cuando los datos personales hayan sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable le deberá informar tal circunstancia, para que también proceda a rectificar o cancelar, según sea el caso.
68. Por su parte, en el también reclamado artículo 105 del Reglamento de la LFPDPPP, se prevé que la cancelación implica el cese en el tratamiento por parte del responsable, a partir de su bloqueo y posterior supresión.
69. Se establece en el artículo 107 del reglamento controvertido que de resultar procedente la cancelación el responsable debe: a) establecer un periodo de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual, y notificarlo al titular o a su representante en la respuesta a la solicitud de cancelación que al efecto emita; b) atender las medidas de seguridad adecuadas para el bloqueo; c) llevar a cabo el bloqueo en el plazo de quince días que establece el diverso artículo 32 de la ley y, finalmente, d) transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente bajo las medidas de seguridad que previamente estableció.
70. En el artículo 108 del propio ordenamiento reglamentario se dispone que el bloqueo tiene como propósito impedir el tratamiento de los datos personales, a excepción del almacenamiento o posible acceso, salvo que alguna disposición legal prevea lo contrario y, reitera, que el periodo de bloqueo será hasta el plazo de prescripción legal o contractual correspondiente.

71. Como se advierte, conforme a las normas aplicables y, en su caso, las reclamadas, el bloqueo de datos personales es aquel período en que el particular responsable del tratamiento de datos personales los identifica y conserva o almacena con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual aplicables.
72. Las normas son claras al establecer que, durante ese lapso, que inicia una vez que se accede a la solicitud de cancelación del tratamiento de datos personales, el particular responsable deja de tratarlos, con excepción de la acción de almacenamiento o conservación y eventual acceso a entes competentes, con la única finalidad de determinar posibles responsabilidades ocurridas cuando aún los trataba y por el plazo legal o contractual de prescripción, según sea el caso. Transcurrido dicho plazo, los datos personales son suprimidos bajo las medidas de seguridad previamente establecidas.
73. Lo anterior evidencia que, contrario a lo afirmado por la quejosa, las normas reclamadas no prevén el almacenamiento indeterminado y prolongado de sus datos personales, sino que ello se limita al plazo legal o contractual de prescripción aplicable.
74. Es cierto que, en el caso, es posible que ese lapso pudiera ser prolongado porque hasta antes de la cancelación de datos personales, con cada operación bancaria no presencial que realizó la quejosa y en virtud de la cual se geolocalizaba las operaciones que realizó, iniciaba, por cada una, el plazo de prescripción. Aunque, esa consecuencia es atribuible a la aplicación de las normas reclamadas, no así a su contenido, por ello no asiste razón a la promovente al afirmar que el lapso de bloqueo es indeterminado pues, como ya se vio, está limitado al plazo de prescripción legal o contractual aplicable.
75. Además, esta Segunda Sala considera que tanto la existencia como duración del período de bloqueo se encuentran plenamente justificados.
76. Conforme a la normatividad y doctrina aplicable en materia de protección de datos personales, los responsables del tratamiento sean sujetos obligados o, como en este caso, particulares, deben cumplir distintos principios entre los que se encuentra el de calidad en virtud del cual deben, entre otras cosas, limitar el período de conservación de los datos al mínimo necesario, de manera que cuando hayan dejado de ser indispensables para el cumplimiento de las finalidades que legitimaron su tratamiento deben ser cancelados o convertidos en anónimos.
77. Ese período de conservación incluye no sólo el tiempo requerido para cumplir las finalidades del tratamiento, sino también los plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables, así como el del bloqueo, pues durante este último lapso el responsable sólo puede tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento que en general les dio.
78. De esa manera, **el bloqueo es para determinar posibles responsabilidades**, es decir, su existencia se encuentra plenamente justificada, porque es para determinar posibles responsabilidades vinculadas con el tratamiento que se dio a los datos personales proporcionados por el titular.
79. En otras palabras, el período del bloqueo no obedece a un capricho del legislador o del responsable del tratamiento de datos personales, sino al hecho de que durante

ese tratamiento pudieron ocurrir situaciones que pueden generar responsabilidades de terceros o del propio responsable y que deben ser sancionadas, todo ello en beneficio del titular de la información.

80. Lo expuesto también es útil para entender por qué el período de bloqueo dura el plazo de prescripción legal o contractual aplicable, justamente porque durante ese lapso serán verificables y sancionables las posibles conductas indebidas o ilícitas ocurridas durante el tratamiento y que, generalmente, están sujetas al plazo de prescripción.

81. Tan es así que, tratándose de los plazos de prescripción legal, las propias leyes de protección de datos personales remiten a las leyes de las materias o sustantivas conducentes para ese efecto.
82. Sobre todo, no debe perderse de vista que, durante el período correspondiente, son bloqueados los datos personales, de manera que no pueden ser tratados por el responsable sino única y exclusivamente para su almacenamiento y posible acceso en caso de que se verifique algún tipo de responsabilidad de la que se viene hablando.
83. En consecuencia, es inexacto lo que pretende hacer ver la quejosa en el sentido de que las normas reclamadas permiten que durante el plazo de bloqueo el responsable puede seguir tratando los datos personales de manera indiscriminada, pues, como ya se dijo, sólo es para su conservación y eventual acceso ante la detección de cierta responsabilidad.
84. Por tanto, esta Segunda Sala llega a la convicción de que los artículos 25 de la LFPDPPP y 105 y 107 de su reglamento, son acordes al orden constitucional.
85. En las relatadas circunstancias, ante lo infundado de los argumentos de la quejosa, lo que se impone es **negar el amparo** contra los artículos 25 de la LFPDPPP, 105 y 107 de su reglamento.

V.2. GEOLOCALIZACIÓN DE DISPOSITIVOS CON ACCESO A INTERNET

86. En su segundo concepto de violación, la promovente afirma que las disposiciones reclamadas violan los derechos a la privacidad, protección de datos personales, acceso a las tecnologías de la información y comunicación, así como de libertad de expresión, porque establecen la obligación de las instituciones de crédito de recabar y almacenar de manera masiva, indiscriminada, obligatoria y prolongada los datos de geolocalización de todas las personas usuarias de servicios financieros en línea, así como su transferencia sin control judicial a diversas autoridades.
87. Explica que tales normas condicionan el acceso y utilización de servicios financieros en línea al otorgamiento del “consentimiento” para el tratamiento de datos de geolocalización de los dispositivos en los que se realicen operaciones y/o utilicen servicios bancarios, siendo que ese consentimiento es irreal pues está condicionado al uso o no de la plataforma.
88. Sostiene que, como las normas reclamadas prevén como obligación la recopilación y almacenamiento de datos de localización geográfica en tiempo real de dispositivos al utilizar servicios de banca electrónica, es claro que el tratamiento de esos datos

del cliente o usuario constituye una interferencia en el derecho a la privacidad o intimidad y una invasión al derecho de protección de datos personales, en tanto que esa información constituye datos personales sensibles, de conformidad con lo establecido en el artículo 3o., fracciones V y VI, de la LFPDPPP.

89. Agrega que las disposiciones reclamadas no superan el test de proporcionalidad porque, si bien, pueden tener un fin constitucionalmente válido como es la prevención y persecución de delitos, lo objetivamente cierto es que no existe prueba demostrativa de que la geolocalización sirva para cumplir dichos fines, aunado a que pueden existir medidas menos lesivas para los derechos en cuestión y, finalmente, porque el grado de afectación que provocan es mucho mayor que el grado de satisfacción del fin perseguido.
90. De ahí que afirme que las disposiciones que reclama de la Resolución que reforma, adiciona y deroga diversas de las disposiciones de carácter general a que se refiere el artículo 115 de la LIC, publicada en el DOF el veintidós de marzo del dos mil diecinueve, son contrarias al orden constitucional.
91. Para resolver sus argumentos, se debe tener en cuenta que el artículo 6o., apartado A, fracción I, de la CPEUM establece que toda información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes de la Unión, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en los tres ámbitos de gobierno, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. Asimismo, que en la interpretación de tal derecho debe prevalecer el principio de máxima publicidad.
92. En contrapartida, la fracción II del propio apartado A, dispone que la información que se refiere a **la vida privada y los datos personales** será protegida en los términos y con las excepciones que fijen las leyes.
93. Cabe recordar que el artículo 16, párrafo segundo, constitucional establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y su cancelación, así como a expresar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
94. Las dos últimas disposiciones son el fundamento constitucional de la vida privada y de la protección de los denominados datos personales, los cuales no son absolutos, pueden existir excepciones o restricciones, siempre y cuando estén reguladas en las leyes y atiendan a razones de seguridad nacional, disposiciones de orden y salud públicas o para proteger los derechos de terceros.
95. Al resolver la acción de inconstitucionalidad 101/2017, en sesión de siete de mayo del dos mil diecinueve, el Pleno de esta SCJN interpretó tales disposiciones y, en específico, la reforma en materia de transparencia y acceso a la información pública de siete de febrero del dos mil catorce, en términos siguientes:

A. La citada reforma marcó un hito en el desarrollo del derecho a la protección de datos en nuestro país.

B. Estableció bases constitucionales para dotar al sector público federal de un régimen legal en materia de protección de datos, aunado a que abrió la posibilidad

de emitir una ley general que desarrollara los principios, bases y procedimientos que de manera uniforme regule tal prerrogativa en los tres niveles de gobierno.

C. Estableció que con la adición al artículo 73, fracción XXIX-S, constitucional, se buscó dotar a los habitantes de este país de leyes de vanguardia que proporcionen herramientas jurídicas a fin de limitar los actos de autoridad, en específico, para ejercer plenamente **el derecho a la protección de datos personales** que no es más que la **autodeterminación informativa**, de manera que cada persona pueda decidir libremente sobre el uso y destino de sus datos personales, teniendo en todo momento derecho a acceder, rectificar, cancelar y oponerse legítimamente a su tratamiento.

96. Por su parte, en la acción de inconstitucionalidad 82/2021, resuelta en sesión de veintiséis de febrero del dos mil veintidós, la SCJN analizó la constitucionalidad de diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) en relación con la creación y regulación del Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT).
97. El Pleno reconoció que **el derecho a la privacidad** protege esa esfera del individuo contra las intromisiones externas que limitan la capacidad para tomar ciertas decisiones a través de las que se ejerce la autonomía personal.
98. Indicó que, dentro del ámbito general de protección del derecho en comento, se identificó el denominado **derecho a la intimidad**, que se integra por los aspectos más personales de la vida y del entorno familiar de un individuo, de manera que el concepto de vida privada comprende a la intimidad como núcleo protegido con mayor fuerza porque se entiende como esencial en la configuración de la persona, esto es, la vida privada es lo reservado y la intimidad lo radicalmente vedado.
99. Posteriormente, al hablar del derecho de protección de datos personales, el Pleno identificó diversos instrumentos internacionales que son orientadores en la materia, tales como los Principios Actualizados sobre la Privacidad y la Protección de los Datos Personales adoptados por el Comité Jurídico Interamericano. Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, así como el Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.
100. Dijo que dichos ordenamientos son coincidentes en definir los datos personales como la información que identifica o puede, de manera razonable, identificar a una persona física de forma directa o indirecta, especialmente por referencia a un número de identificación, datos de localización, un identificador en línea o a uno o más factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social, incluyendo información expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otra manera.
101. Informó que tales instrumentos ubican a los **datos personales sensibles** como una categoría estrecha que incluye la información o aspectos más íntimos de las personas y que, según el contexto cultural, social o político podría abarcar los datos relacionados con la salud personal, las preferencias sexuales o vida sexual, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas, el origen racial o étnico, información sobre cuentas bancarias,

documentos oficiales, información recopilada de niños y niñas, o bien, la **geolocalización personal**.

102. Finalmente, se estableció que, si bien los derechos a la privacidad, intimidad y protección de datos personales son distinguibles y autónomos, se encuentran estrechamente vinculados, pues la interdependencia que existe entre sus respectivos ámbitos de tutela da lugar a un bloque de defensa tendente a proteger al individuo de cualquier interferencia o molestia que pudiera efectuarse sobre la esfera de su privacidad, provengan de particulares o del propio Estado.
103. Como se ve, a través de dichos precedentes, esta SCJN ha diferenciado las prerrogativas que la quejosa afirma son violadas por las disposiciones reclamadas, esto es, los derechos a la privacidad, intimidad y protección de datos personales. A pesar de ello, los tres conforman un bloque de defensa o protección que se va ampliando o reduciendo, dependiendo del tipo de información o dato de que se trate, esto es, si se vincula con la privacidad, la intimidad, o bien, con los datos personales o sensibles de sus titulares.
104. Ahora, las disposiciones reclamadas están contenidas en la Resolución que reforma, adiciona y deroga diversas de las Disposiciones de carácter general a que se refiere el artículo 115 de la LIC, publicada en el DOF el veintidós de marzo del dos mil diecinueve.
105. En este sentido, conviene traer a cuenta que en el artículo 115, cuarto párrafo, de la LIC se establece que las instituciones de crédito, en términos de las disposiciones de carácter general que emita la SHCP, previa opinión de la Comisión Nacional Bancaria y de Valores (CNBV), están obligadas a establecer medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión de los delitos previstos en los artículos 139 o 148 Bis del Código Penal Federal (terrorismo) o que pudieran ubicarse en los supuestos del artículo 400 Bis (operaciones con recursos de procedencia ilícita) del propio ordenamiento, así como a presentar a la SHCP, por conducto de la CNBV, los reportes ahí precisados.
106. Incluso, en su párrafo sexto se establece que en dichas disposiciones la SHCP emitirá los lineamientos sobre el procedimiento y criterios que las instituciones de crédito deben observar para el adecuado conocimiento de sus clientes y usuarios, para lo cual deberán considerar los antecedentes, condiciones específicas, actividad económica o profesional y las plazas en que operen (inciso a); la información y documentación que las instituciones recaben para la apertura de cuentas o celebración de contratos relativos a las operaciones y servicios que presten y que acredite plenamente la identidad de sus clientes (inciso b); y la forma en que las propias instituciones deben resguardar y garantizar la seguridad de la información y documentación relativas a la identificación de sus clientes y usuarios o quienes lo hayan sido, así como la de aquellos actos, operaciones y servicios reportados conforme a ese artículo (inciso c).
107. Con base en lo anterior, la SHCP emitió las disposiciones de carácter general, cuya resolución que reforma, adiciona y deroga diversas de ellas, publicada en el DOF el veintidós de marzo del dos mil diecinueve, reclamó la quejosa en el juicio de amparo de origen.
108. Al efecto, en la disposición 2, fracción XVI, se define el concepto de **geolocalización** como las coordenadas geográficas de latitud y longitud en que se

encuentre el **dispositivo**, esto es, el equipo que permite acceder a internet y que puede ser utilizado para abrir cuentas o celebrar contratos, así como realizar operaciones.

109. En la disposición 4 se dispone que las entidades, esto es las instituciones de crédito, deben integrar y conservar un expediente de identificación de cada uno de sus clientes previamente, cuando de manera presencial abran una cuenta o celebren un contrato para realizar operaciones de cualquier tipo. Se precisa que, para integrar los expedientes de identificación de los clientes, deben cumplir, cuando menos, tratándose de, entre otras, personas físicas que declaren ser de nacionalidad mexicana, con la información siguiente:

a. Los datos de identificación tales como: nombre completo sin abreviaturas, género, fecha y lugar de nacimiento, nacionalidad, ocupación, profesión, actividad o giro del negocio, domicilio completo del lugar de residencia, número(s) de teléfono; correo electrónico, Clave Única de Registro de Población, clave del Registro Federal de Contribuyentes (con homoclave), número de identificación fiscal y/o equivalente, así como el país o países que los asignaron, número de serie de la Firma Electrónica Avanzada.

b. Copia simple de la identificación personal y de los documentos que acrediten los datos anteriores; declaración de la persona física en la que conste que actúa para esos efectos a nombre y por cuenta propia o por cuenta de un tercero, según sea el caso. En caso de que la persona física declare que actúa por cuenta de un tercero, la entidad debe observar lo dispuesto en la fracción VI de dicha disposición respecto del propietario real de los recursos involucrados en la cuenta o contrato correspondiente; copia simple de la carta poder o de la copia certificada del documento expedido por fedatario público en los casos en que la persona física actúe como apoderado de otra persona.

110. Conforme a la disposición 4 Ter reclamada, las entidades que abran una cuenta o celebren un contrato a través de dispositivos de forma no presencial, además de los datos de identificación antes mencionados o los aplicables, según sea el caso, **deben requerir y obtener de sus clientes, previo consentimiento, la geolocalización del dispositivo desde el cual realicen esa operación**, así como la demás información ahí precisada.

111. En el párrafo segundo de la fracción VII reclamada de dicha disposición 4 Ter, se prevé que las entidades **no deben llevar a cabo la apertura de la cuenta o la celebración del contrato de forma no presencial con los clientes, cuando no recaben el dato relativo a la geolocalización.**

112. Por su parte, en el numeral 10 se prohíbe a las entidades celebrar contratos o mantener cuentas anónimas, bajo nombres ficticios o en las que no se pueda identificar al cliente o propietario real, por lo que únicamente pueden celebrar operaciones con sus clientes cuando hayan cumplido los requisitos de identificación, conforme a tales disposiciones.

113. En la también reclamada disposición 16 Bis, párrafos segundo y tercero, se establece que las entidades que opten por integrar el expediente de identificación del usuario de forma no presencial y a través de medios electrónicos, ópticos o de

cualquier otra tecnología, deben requerir y obtener, previo su consentimiento, la geolocalización del dispositivo desde el cual celebre la operación, así como su correo electrónico. En caso de no recabar esa información, tienen prohibido celebrar operaciones con usuarios de forma no presencial.

114. Las disposiciones 21-1 a 21-6 pertenecen al Capítulo II Bis denominado Enfoque basado en riesgos y prevén, entre otras cosas, el deber de las entidades de diseñar e implementar una metodología para llevar a cabo una evaluación de riesgos a los que se encuentran expuestas derivado de sus productos, servicios, clientes, usuarios, países o áreas geográficas, transacciones y canales de envío o distribución con los que operan.
115. El Capítulo III Política de conocimiento del cliente y del usuario, contiene la disposición 24, en cuyo párrafo primero se dispone que el perfil transaccional de cada uno de los clientes estará basado en la información que éstos proporcionen a la entidad y, en su caso, en aquella con que cuente la misma, respecto del monto, número, tipo, naturaleza y frecuencia de las operaciones que comúnmente realizan, el origen y destino de los recursos involucrados, así como en el conocimiento que tenga el empleado o funcionario de la entidad respecto de su cartera de clientes, y en los demás elementos y criterios que determinen las propias instituciones.
116. Se prevé en el párrafo segundo reclamado que, tratándose de operaciones realizadas de forma no presencial, también de los elementos para determinar el perfil transaccional del cliente antes señalados, se deberá tomar en cuenta la geolocalización del dispositivo donde se lleve a cabo dicha operación.
117. En la disposición 25 se establece que la aplicación de la política de conocimiento del cliente se debe basar en el grado de riesgo que represente, de tal manera que, cuando el grado sea mayor, la entidad debe recabar más información sobre su actividad preponderante, así como realizar una supervisión más estricta a su comportamiento transaccional.
118. Ahora bien, en la disposición 25 Bis se relaciona con el establecimiento del grado de riesgo de los clientes, pudiendo mediar entre el bajo y alto tantos peldaños como la entidad considere necesario, debiendo ser diferenciables entre sí. Para determinar el grado de riesgo inicial, las instituciones de crédito deben considerar, al menos durante los seis primeros meses siguientes al inicio de la relación comercial, la información que proporcione cada uno de sus clientes, debiendo evaluar ese riesgo cada seis meses, y ser más frecuente cuanto más alto sea el grado de riesgo.
119. En el párrafo cuarto reclamado de la disposición 25 Bis se dispone que, tratándose de la apertura de cuentas o celebración de contratos de forma no presencial, las entidades deben considerar la información de la geolocalización, previo consentimiento del cliente, del dispositivo desde el cual realice la operación, actividad o servicio contratado.
120. En los últimos dos párrafos de la norma en comento se prevé que las entidades aplicarán a sus clientes que hayan sido catalogados como de grado de riesgo alto, así como a los nuevos que reúnan tal carácter, cuestionarios de identificación que permitan obtener mayor información sobre el origen y destino de los recursos y las actividades y operaciones que realizan o que pretendan llevar a cabo, los cuales podrán realizarse vía no presencial, por medios digitales o electrónicos, con el fin de procurar la veracidad y seguridad en su elaboración, los cuales en todo caso

deberán contener el consentimiento a que se refiere la disposición 4ª Ter, de quien los suscribe, esto es, el consentimiento para su geolocalización.

121. La disposición 54 prevé la obligación de las instituciones de crédito de proporcionar a la SHCP, por conducto de la CNBV, toda la información y documentación que les requiera, incluyendo la que contenga imágenes, relacionada con los reportes ahí regulados y, en el evento de que la dependencia requiera a una entidad copia del expediente de identificación de alguno de sus clientes o usuarios, ésta debe remitirle todos los datos y copia de toda la documentación que, conforme a lo previsto en las disposiciones, deba formar parte del expediente respectivo. Si la Secretaría requiere otra información relacionada, la entidad deberá presentarle toda la demás información y copia de toda la documentación que, sobre dicho cliente o usuario, obre en su poder.

122. En el último párrafo de esa disposición se ordena que la información y documentación requerida por la CNBV deberá ser presentada directamente en la unidad administrativa que para tales efectos se designe, y deberá ir contenida en sobre cerrado a fin de evitar que personas ajenas a dicha unidad tengan acceso a la referida información y documentación.
123. Así, tenemos que en las disposiciones reclamadas se establecen obligaciones a cargo de las entidades o instituciones de crédito en el sentido de recabar de sus clientes el consentimiento para su geolocalización cuando realicen operaciones a distancia a través de dispositivos, entendiéndose por estos cualquier equipo que permita acceder a internet y que puede ser utilizado para abrir cuentas, celebrar contratos y realizar operaciones (activas, pasivas, de servicios y las análogas y conexas a las anteriores, así como aquellas con activos virtuales que, conforme a las leyes que rigen su funcionamiento, celebren las entidades, con excepción de los descuentos que realicen las instituciones de banca de desarrollo).
124. El resto de las disposiciones comentadas dan el contexto en el que se desarrollan las normas controvertidas y dejan ver tanto las atribuciones como las obligaciones y prohibiciones que tienen las instituciones de crédito al realizar sus operaciones presenciales o a distancia.
125. Como ya se dijo, en su demanda de amparo, la quejosa reclama, en esencia, que las disposiciones reclamadas violan los derechos a la privacidad, intimidad y de protección de datos personales, porque el hecho de que las instituciones de crédito estén obligadas a geolocalizar su dispositivo cuando abre cuentas o realiza operaciones no presenciales, implica una intromisión a su vida e información privada, pues incluso a través de ella se pueden conocer sus movimientos, ubicaciones y demás aspectos que permiten identificarla. Es más, la quejosa considera que la geolocalización de su dispositivo constituye un dato personal sensible.
126. Al respecto, es de señalar que en el artículo 3o., fracción V, de la LFPDPPP, aplicable al caso, se define a los datos personales como cualquier información concerniente a una persona física identificada o identificable, en efecto, permite identificar o hacer identificable a cierta persona ya sea de manera directa o indirecta.

127. Conforme al mismo artículo 3o., fracción VI, del propio ordenamiento legal, son datos personales sensibles aquéllos que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave. En particular, se consideran sensibles los que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.
128. Como se dijo, la geolocalización o localización geográfica consiste en las coordenadas geográficas de latitud y longitud en que se encuentra el dispositivo a través del cual se abre una cuenta o se realiza una operación bancaria no presencial, implica información acerca de la ubicación geográfica en tiempo real del dispositivo a través del cual el cliente o el usuario, según sea el caso, realiza alguna operación bancaria.
129. Si bien, la información que arroja esa geolocalización se reduce a coordenadas de latitud y longitud, lo cierto es que a través de ellas se puede establecer un patrón de comportamiento o, incluso, un estilo de vida que permita identificar o hacer identificable a la portadora o tenedora de ese dispositivo.
130. Tal circunstancia evidencia que dicha geolocalización constituye un dato personal pues permite identificar o hacer identificable a cierta persona mediante el conocimiento de la ubicación geográfica del dispositivo utilizado para realizar una operación bancaria no presencial.
131. No obstante, contrario a lo afirmado por la quejosa, esa información no es un dato personal sensible porque, en principio, no lo reconoce como tal la ley federal aplicable y, si bien, es cierto los datos que considera sensibles son enunciados de manera ejemplificativa mas no limitativa, lo cierto es que tampoco se le puede dotar de esa naturaleza por la afectación que puede conllevar. Para considerar que un dato personal es sensible es necesario que afecte la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave.
132. Si bien, a través de la geolocalización del dispositivo utilizado para realizar ese tipo de operaciones se puede identificar o hacer identificable a una persona, lo cierto es que, de suyo, no afecta su esfera más íntima, a grado tal como lo hace, por ejemplo, los datos genéticos, el estado de salud, la orientación sexual, los datos biométricos y en general toda aquella información que le es inherente y que lo hace vulnerable en el ámbito más íntimo.
133. De igual manera, el uso indebido de la ubicación geográfica del aludido dispositivo tampoco ocasiona forzosa y necesariamente actos de discriminación, o bien, poner en riesgo grave a la persona que lo detente, pues debe recordarse que lo que se ubica geográficamente o se geolocaliza es el dispositivo con acceso a internet a través del que se realizan operaciones bancarias no presenciales y únicamente en cuanto el momento en que se realiza la misma.
134. Esto es, lo que se geolocaliza es el aludido dispositivo, no la persona y si bien, a través del conocimiento de esas coordenadas se puede establecer un patrón de vida del individuo que lo utiliza haciéndolo identificable, lo cierto es que, de suyo, no implica la localización personal, sino del dispositivo con acceso a internet y únicamente en el momento que se lleva a cabo esta.

135. Incluso, esta interpretación es acorde con los precedentes emitidos por esta SCJN en materia penal, en los que se estableció que lo que se geolocaliza es el dispositivo móvil utilizado para la perpetración de ciertos ilícitos, o bien, en materia de telecomunicaciones en que se ha precisado que la geolocalización permitida constitucionalmente es aquella vinculada con dispositivos móviles siempre que se relacionen con aspectos de procuración de justicia.
136. Tales criterios de interpretación se encuentran, por ejemplo, en las acciones de inconstitucionalidad 32/2012, resuelta por el Tribunal Pleno el dieciséis de enero del dos mil catorce, la diversa 10/2014 y su acumulada 11/2014, resueltas en sesión plenaria de veintidós de marzo del dos mil dieciocho, así como en el amparo en revisión 964/2015, resuelto por esta Segunda Sala en sesión de cuatro de mayo del dos mil dieciséis.
137. En este punto es necesario precisar que en el asunto que nos ocupa lo que se geolocaliza de momento a momento es el dispositivo con acceso a internet a través del cual se realizan operaciones bancarias no presenciales, mismo que no necesariamente se identifica con un teléfono móvil, sino que puede ser una desktop, una laptop, un iPad o tableta, en fin, cualquier dispositivo o aparato electrónico que tenga acceso a dicha red internacional y a través del cual se puedan hacer movimientos bancarios.
138. Tal circunstancia corrobora que la información de geolocalización de ese tipo de dispositivos puede constituir un dato personal, pero no sensible, porque no implica la intromisión en el ámbito más íntimo de una persona, no conlleva forzosa y necesariamente actos de discriminación ni puesta en peligro, sino que a través de ella, en su caso, se pueden detectar patrones de actividades, estilo de vida o la frecuente visita de lugares cuyo conocimiento permita identificar o hacer identificable a una persona.
139. En consecuencia, la geolocalización que establece y regula las normas reclamadas se puede constituir como un dato personal, pero no sensible como equivocadamente alega la quejosa.
140. No pasa inadvertido que, como se dijo al comentar el precedente del PANAUT, los diversos instrumentos internacionales ahí relacionados consideran a la geolocalización personal como un dato personal sensible, pese a lo cual, en la especie, se insiste, la geolocalización no es como tal de la persona, sino del dispositivo con acceso a internet que utiliza para realizar operaciones bancarias a distancia y ésta se lleva a cabo únicamente al momento de realizar la operación.
141. Lo anterior de ninguna manera es un contrasentido. Si bien, por ejemplo, el teléfono móvil puede ser utilizado por una persona constantemente para realizar ese tipo de operaciones y generalmente lo lleva consigo, lo objetivamente cierto es que ese entendimiento parte de sólo considerar al teléfono móvil como el dispositivo que refieren las disposiciones reclamadas, siendo que ese concepto es definido en términos amplios, esto es, como el equipo que permite acceder a internet y que puede ser utilizado para abrir cuentas o celebrar contratos, así como realizar operaciones no presenciales.

142. De ahí que el hecho de que en aquel precedente se haya reconocido que en virtud de aquellos ordenamientos la geolocalización personal es un dato personal sensible, no colisiona con lo aquí establecido en cuanto a la geolocalización del dispositivo a que aluden los preceptos controvertidos.
143. Ahora bien, como se desprende de su lectura, las disposiciones reclamadas obligan a las entidades o instituciones de crédito a obtener, previo consentimiento de sus clientes o usuarios, la geolocalización de los dispositivos mediante los que realizan operaciones bancarias no presenciales. A través del conocimiento de esa información se puede identificar o hacer identificable a una persona, de modo que pudiere incidir en la protección de datos personales que implican la esfera privada de un individuo.
144. En este punto conviene traer a colación la parte considerativa de la Resolución en estudio en la que se indicó lo siguiente:

Que durante el periodo 2016-2017, México fue evaluado en el marco de la Cuarta Ronda de Evaluación Mutua del Grupo de Acción Financiera (GAFI), con el fin de examinar su nivel de cumplimiento en los estándares internacionales en materia de prevención de lavado de dinero y financiamiento al terrorismo;

Que, derivado de lo anterior, el 3 de enero de 2018 el GAFI publicó el "Informe de Evaluación Mutua" mediante el cual dicho ente intergubernamental realizó a México diversas recomendaciones con el fin de fortalecer su régimen de prevención de lavado de dinero y financiamiento al terrorismo;

Que por lo anterior, la Secretaría de Hacienda y Crédito Público ha considerado realizar diversas modificaciones a las disposiciones de carácter general que establecen los criterios y procedimientos mínimos en materia de prevención de lavado de dinero y financiamiento al terrorismo al sector bancario, esto con el objeto de atender las recomendaciones del GAFI y fortalecer el régimen en la materia;

Que, adicionalmente a la reforma realizada el 24 de febrero de 2017 a las disposiciones de carácter general en materia de prevención de lavado de dinero y financiamiento al terrorismo aplicables al sector bancario, para coadyuvar a mejorar el cumplimiento de las Recomendaciones 1 y 10 del GAFI, se precisa en el marco legal la prohibición a las instituciones de crédito para llevar a cabo medidas simplificadas de identificación de sus clientes o usuarios cuando tengan sospecha de que los recursos, bienes o valores que dichos clientes o usuarios pretendan usar para realizar una operación, pudieran estar relacionados con el lavado de dinero o financiamiento al terrorismo;

Que asimismo, en apego a la Recomendación 10 del GAFI, resulta necesario fortalecer el marco legal respecto a la política de identificación y conocimiento del cliente o usuario para el sector bancario, estableciéndose los supuestos en los que podrán suspender el proceso de identificación, con el fin de prevenir la comisión de delitos de lavado de dinero y financiamiento al terrorismo, entre otros; y en su caso, remitir a la autoridad competente el reporte de operación inusual respectivo;

Que, para atender de mejor forma la Recomendación 12 del GAFI, es conveniente establecer que las instituciones de crédito determinen si los propietarios reales de sus clientes o usuarios tienen el carácter de personas políticamente expuestas, ya sea nacionales o extranjeros conforme a las disposiciones aplicables, para estar en posibilidad de aplicar las medidas de debida diligencia del cliente adecuadas o reforzadas;

Que, conforme a la Recomendación 16 del GAFI, relacionada con las transferencias electrónicas de fondos, en consideración a las modificaciones previstas para los formatos de mensajes estandarizados más utilizados por las entidades financieras en el mercado internacional para dichas operaciones, resulta necesario fortalecer la política de identificación del cliente o usuario de la institución de crédito, con el fin de conocer con mayor precisión la información del ordenante y beneficiario de la

transferencia de que se trate, para detectar y, en su caso, evitar la comisión de delitos de operaciones con recursos de procedencia ilícita y financiamiento al terrorismo, por lo cual, es necesario que las instituciones de crédito identifiquen, con independencia del monto de la operación, a los clientes o usuarios que solicitan enviar las respectivas transferencias, así como a los beneficiarios de estas, particularmente al emitir las respectivas órdenes de transferencia o bien, a los ordenantes de las respectivas órdenes de transferencias internacionales que reciban y, como en otros casos, mantengan dicha información en los plazos en los que se encuentran obligadas y a disposición de la autoridad competente, además de obligar a las referidas entidades a establecer criterios en sus respectivos manuales que les permitan fortalecer, con un enfoque basado en riesgos, su régimen de prevención de lavado de dinero y financiamiento al terrorismo sobre esta materia;

Que, por otro lado, dado que las instituciones de crédito pueden prestar servicios financieros a través de nuevas tecnologías, mismas que han sido reconocidas por el Gobierno Mexicano con la emisión de la Ley para Regular las Instituciones de Tecnología Financiera y sus disposiciones secundarias, en apego a la Recomendación 15 del GAFI y a lo señalado en el Informe del 3 de enero de 2018, es necesario que estas evalúen el riesgo de prestar servicios financieros a través de las citadas tecnologías, por lo que resulta conveniente establecer tal obligación, previo a su implementación y desarrollo, así como para su monitoreo;

Que, asimismo, la Ley mencionada en el considerando anterior autoriza a las instituciones de crédito para operar con activos virtuales, por lo anterior, es preciso establecer la política de identificación y conocimiento del cliente cuando operen con dichos activos virtuales, los reportes y, en su caso, el intercambio de información con otras entidades financieras autorizadas para ello;

Que, aun y cuando actualmente las instituciones de crédito cumplen con la obligación de la debida diligencia del cliente de forma presencial y tradicional, salvo algunas excepciones reconocidas en la norma, ante la existencia de la era digital, las nuevas tecnologías y los medios electrónicos, en la integración, conservación, mantenimiento, verificación, etc., de datos, información y documentos, resulta necesario, al igual que con otros participantes regulados en la materia, reconocer la posibilidad legal de que las instituciones de crédito puedan cumplir con sus obligaciones en materia de prevención de lavado de dinero y financiamiento al terrorismo a través de dichos medios electrónicos, desde luego con la obligación de que cumplan con las normas aplicables al efecto, para que tengan el valor jurídico que en derecho corresponde;

Que, con la finalidad de priorizar esfuerzos y recursos en las nuevas obligaciones establecidas en la presente resolución, se estima conveniente eliminar la obligación para las instituciones de crédito de enviar el informe de capacitación, sin que ello implique que no deban contar con dicha capacitación, y

Que una vez escuchada la opinión de la Comisión Nacional Bancaria y de Valores, he tenido a bien emitir la siguiente: (...)

145. Del texto transcrito se advierte que la modificación a la resolución mencionada deriva de diversas recomendaciones que realizó el Grupo de Acción Financiera Internacional (GAFI) que es un ente intergubernamental cuyo objetivo es establecer estándares y promover la implementación efectiva de medidas legales, regulatorias y operativas para combatir el lavado de activos, el financiamiento al terrorismo, a la proliferación de armas de destrucción masiva y otras amenazas a la integridad del sistema financiero internacional, con motivo de la evaluación realizada a México en el marco de la Cuarta Ronda de Evaluación Mutua en el período dos mil dieciséis – dos mil diecisiete.
146. Las recomendaciones que el ente hacendario tomó en cuenta para modificar la resolución mencionada son las identificadas con los numerales 1 (evaluación de

riesgo y aplicación de un enfoque basado en el riesgo); 10 (debida diligencia del cliente); 12 (personas expuestas políticamente); 15 (nuevas tecnologías); y 16 (transferencias electrónicas), del total de cuarenta que emite dicho órgano.

147. Para efectos de este estudio, conviene hacer patente que a través de la recomendación 10, el GAFI señaló lo siguiente:

Debe prohibirse a las instituciones financieras que mantengan cuentas anónimas o cuentas con nombres obviamente ficticios.

Debe exigirse a las instituciones financieras que emprendan medidas de Debida Diligencia del Cliente (DDC) cuando: (i) establecen relaciones comerciales; (ii) realizan transacciones ocasionales: (i) por encima del umbral aplicable designado (USD/EUR 15,000); o (ii) están ante transferencias electrónicas en las circunstancias que aborda la Nota Interpretativa de la Recomendación 16; (iii) existe una sospecha de lavado de activos o financiamiento del terrorismo; o (iv) la institución financiera tiene dudas sobre la veracidad o idoneidad de los datos de identificación sobre el cliente obtenidos previamente.

El principio de que las instituciones financieras deben llevar a cabo la DDC debe plasmarse en ley. Cada país puede determinar cómo impone obligaciones específicas de DDC, ya sea mediante ley o medios coercitivos.

Las medidas de DDC a tomar son las siguientes: (a) Identificar al cliente y verificar la identidad del cliente utilizando documentos, datos o información confiable, de fuentes independientes. (b) Identificar al beneficiario final y tomar medidas razonables para verificar la identidad del beneficiario final, de manera tal que la institución financiera esté convencida de que conoce quién es el beneficiario final. Para las personas jurídicas y otras estructuras jurídicas, esto debe incluir que las instituciones financieras entiendan la estructura de titularidad y de control del cliente. (c) Entender, y cuando corresponda, obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial. (d) Realizar una debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones que se realicen sean consistentes con el conocimiento que tiene la institución sobre el cliente, su actividad comercial y el perfil de riesgo, incluyendo, cuando sea necesario, la fuente de los fondos.

Debe exigirse a las instituciones financieras que apliquen cada una de las medidas de DDC de los párrafos (a) al (d) anteriores, pero deben determinar el alcance de tales medidas utilizando un enfoque basado en riesgo (EBR) de conformidad con las Notas Interpretativas de esta Recomendación y la Recomendación 1.

Debe exigirse a las instituciones financieras que verifiquen la identidad del cliente y del beneficiario final antes o durante el curso del establecimiento de una relación comercial o al realizar transacciones para clientes ocasionales. Los países pueden permitir a las instituciones financieras que completen la verificación tan pronto como sea razonablemente práctico luego del establecimiento de la relación, cuando los riesgos de lavado de activos y financiamiento del terrorismo se manejen con eficacia y cuando resulte esencial para no interrumpir el curso normal de la actividad.

Si la institución financiera no pudiera cumplir con los requisitos aplicables en los párrafos (a) al (d) anteriores (sujeto a la modificación acorde al alcance de las medidas partiendo de un enfoque basado en riesgo), se le debe exigir a ésta que no abra la cuenta, comience relaciones comerciales o realice la transacción; o se le debe exigir que termine la relación comercial; y debe considerar hacer un reporte de transacciones sospechosas sobre el cliente.

Estos requisitos se deben aplicar a todos los clientes nuevos, aunque las instituciones financieras deben aplicar también esta Recomendación a los clientes existentes atendiendo a la importancia relativa y al riesgo, y deben llevar a cabo una debida diligencia sobre dichas relaciones existentes en los momentos apropiados.

148. Por otra parte, en la recomendación 15 se señaló que “los países y las instituciones financieras deben identificar y evaluar los riesgos de lavado de activos o financiamiento del terrorismo que pudieran surgir con respecto a (a) el desarrollo de nuevos productos y nuevas prácticas comerciales, incluyendo nuevos mecanismos de envío, y (b) el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes. En el caso de las instituciones financieras, esta evaluación del riesgo debe hacerse antes del lanzamiento de los nuevos productos, prácticas comerciales o el uso de tecnologías nuevas o en desarrollo. Los países y las instituciones financieras deben tomar medidas apropiadas para administrar y mitigar esos riesgos” (versión dos mil doce).
149. Vale hacer mención que en la versión del dos mil veintitrés, en suma, posterior a la emisión de las normas reclamadas, se agregó que “para gestionar y mitigar los riesgos que surjan de los activos virtuales, los países deben garantizar que los proveedores de servicios de activos virtuales estén regulados para propósitos ALA/CFT (Anti Lavado de Activos y Contra Financiamiento del Terrorismo), y tengan licencia o registro y estén sujetos a sistemas de monitoreo efectivo y asegurar el cumplimiento de las medidas relevantes requeridos en las Recomendaciones del GAFI”.
150. En la recomendación 16, relativa a las transferencias electrónicas, se señaló que “los países deben asegurar que las instituciones financieras incluyan la información sobre el originador que se requiere, y que ésta sea precisa, así como la información requerida sobre el beneficiario, en las transferencias electrónicas y mensajes relacionados, y que la información permanezca con la transferencia electrónica o mensaje relacionado a lo largo de toda la cadena de pago”.
151. Agregado a lo anterior, que “los países deben asegurar que las instituciones financieras monitoreen las transferencias electrónicas con el propósito de detectar aquéllas que carezcan de la información requerida sobre el originador y/o beneficiario, y tomar las medidas apropiadas. Los países deben asegurar que, en el contexto del procesamiento de las transferencias electrónicas, las instituciones financieras tomen medidas para congelar y deben prohibir la realización de transacciones con personas y entidades designadas, según las obligaciones plasmadas en las resoluciones pertinentes del Consejo de Seguridad de las Naciones Unidas, como la Resolución 1267 (1999) y sus resoluciones sucesoras y la Resolución 1373 (2001), relativa a la prevención y represión del terrorismo y el financiamiento del terrorismo”.
152. De la lectura del documento que contiene dichas recomendaciones, así como de las específicas antes transcritas, se advierte que están dirigidas a que los miembros del Grupo de Acción Financiera (GAFI) implementen diversas medidas tendentes a combatir el lavado de activos, el financiamiento al terrorismo, a la proliferación de armas de destrucción masiva y, en general, el ataque y vulnerabilidad de sus sistemas financieros. Todas ellas se centran en la necesidad de identificar a las diversas personas que interactúan en dicho sistema, como son los clientes, los beneficiarios, los propietarios y, en general, todos aquéllos que lo utilizan a nivel nacional e internacional.

153. Entonces, es claro que las disposiciones reclamadas tienen como finalidad la seguridad pública y el combate a los delitos antes mencionados, así como la estabilidad de las finanzas públicas y del sistema financiero en su conjunto.
154. Cabe señalar que, conforme a lo dispuesto en el artículo 21 de la CPEUM,¹³ la seguridad pública es una función del Estado a cargo de los distintos ámbitos de gobierno y cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en el propio ordenamiento y en las leyes en la materia.
155. Aún, en el artículo 25, párrafo segundo, constitucional¹⁴ se dispone que el Estado velará por la estabilidad de las finanzas públicas y del sistema financiero para coadyuvar a generar condiciones favorables para el crecimiento económico y el empleo.

¹³ **Artículo 21.** La investigación de los delitos corresponde al Ministerio Público, a las policías y a la Guardia Nacional, en el ámbito de su competencia, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función.

El ejercicio de la acción penal ante los tribunales corresponde al Ministerio Público. La ley determinará los casos en que los particulares podrán ejercer la acción penal ante la autoridad judicial.

La imposición de las penas, su modificación y duración son propias y exclusivas de la autoridad judicial. Compete a la autoridad administrativa la aplicación de sanciones por las infracciones de los reglamentos gubernativos y de policía, las que únicamente consistirán en multa, arresto hasta por treinta y seis horas o en trabajo a favor de la comunidad; pero si el infractor no pagare la multa que se le hubiese impuesto, se permutará esta por el arresto correspondiente, que no excederá en ningún caso de treinta y seis horas.

Si el infractor de los reglamentos gubernativos y de policía fuese jornalero, obrero o trabajador, no podrá ser sancionado con multa mayor del importe de su jornal o salario de un día.

Tratándose de trabajadores no asalariados, la multa que se imponga por infracción de los reglamentos gubernativos y de policía, no excederá del equivalente a un día de su ingreso.

El Ministerio Público podrá considerar criterios de oportunidad para el ejercicio de la acción penal, en los supuestos y condiciones que fije la ley.

El Ejecutivo Federal podrá, con la aprobación del Senado en cada caso, reconocer la jurisdicción de la Corte Penal Internacional.

La seguridad pública es una función del Estado a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, de conformidad con lo dispuesto en el artículo 4o. de esta Constitución que garantiza los deberes reforzados de protección del Estado con las mujeres, adolescentes, niñas y niños; así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en esta Constitución y las leyes en la materia. La seguridad pública comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo y honradez, así como por la perspectiva de género y el respeto a los derechos humanos reconocidos en esta Constitución.

Las instituciones de seguridad pública serán disciplinadas, profesionales y de carácter civil.

El Ministerio Público y las instituciones policiales de los tres órdenes de gobierno, incluida la Guardia Nacional, deben coordinarse entre sí para cumplir los fines de la seguridad pública y conformarán el Sistema Nacional de Seguridad Pública, que estará sujeto a las siguientes bases mínimas:

a) La regulación de la selección, ingreso, formación, permanencia, evaluación, reconocimiento y certificación de los integrantes de las instituciones de seguridad pública. La operación y desarrollo de estas acciones será competencia de la Federación, las entidades federativas y los Municipios en el ámbito de sus respectivas atribuciones.

b) El establecimiento de un sistema nacional de información en seguridad pública a cargo de la Federación al que ésta, las entidades federativas y los Municipios, a través de las dependencias responsables de la seguridad pública, proporcionarán la información de que dispongan en la materia, conforme a la ley. El sistema contendrá también las bases de datos criminalísticos y de personal para las instituciones de seguridad pública. Ninguna persona podrá ingresar a las instituciones de seguridad pública si no ha sido debidamente certificada y registrada en el sistema.

c) La formulación de políticas públicas tendientes a prevenir la comisión de delitos.

d) Se determinará la participación de la comunidad que coadyuvará, entre otros, en los procesos de evaluación de las políticas de prevención del delito así como de las instituciones de seguridad pública.

e) Los fondos de ayuda federal para la seguridad pública, a nivel nacional serán aportados a las entidades federativas y municipios para ser destinados exclusivamente a estos fines.

La Federación contará con la Guardia Nacional, fuerza de seguridad pública, profesional, de carácter permanente e integrada por personal militar con formación policial, dependiente de la secretaría del ramo de defensa nacional, para ejecutar la Estrategia Nacional de Seguridad Pública en el ámbito de su competencia. Los fines de la Guardia Nacional son los señalados en el párrafo noveno de este artículo, la coordinación y colaboración con las entidades federativas y Municipios, así como la salvaguarda de los bienes y recursos de la Nación. La ley determinará la estructura orgánica y de dirección de la Guardia Nacional.

La secretaría del ramo de seguridad pública formulará la Estrategia Nacional de Seguridad Pública, y los programas, políticas y acciones respectivos.

La formación y el desempeño de los integrantes de la Guardia Nacional y de las demás instituciones policiales se regirán por una doctrina policial fundada en el servicio a la sociedad, la disciplina, el respeto a los derechos humanos, al imperio de la ley, al mando superior, y en lo conducente a la perspectiva de género.

¹⁴ **Artículo 25.** Corresponde al Estado la rectoría del desarrollo nacional para garantizar que éste sea integral y sustentable, que fortalezca la Soberanía de la Nación y su régimen democrático y que, mediante la competitividad, el fomento del crecimiento económico y el empleo y una más justa distribución del ingreso y la riqueza, permita el pleno ejercicio de la libertad y la dignidad de los individuos, grupos y clases sociales, cuya seguridad protege esta Constitución. La competitividad se entenderá como el conjunto de condiciones necesarias para generar un mayor crecimiento económico, promoviendo la inversión y la generación de empleo.

El Estado velará por la estabilidad de las finanzas públicas y del sistema financiero para coadyuvar a generar condiciones favorables para el crecimiento económico y el empleo. El Plan Nacional de Desarrollo y los planes estatales y municipales deberán observar dicho principio.

156. Una vez establecido lo anterior, resulta menester entrar al estudio del derecho a la privacidad. Al efecto, debe decirse que con motivo de la reforma en materia de derechos humanos de diez de junio dos mil once, el contenido del artículo 1o. de la CPEUM¹⁵ se amplió al incorporarse en la norma constitucional los derechos internacionales en los que el Estado mexicano es parte. Por ello, todas las autoridades tendrán obligación de respetar no sólo los instrumentos jurídicos nacionales, sino también internacionales.

157. De esta manera, a nivel internacional el derecho a la privacidad se encuentra reconocido y protegido en distintos tratados internacionales de los que el Estado mexicano es parte. Al respecto, la Convención Americana sobre Derechos Humanos, habla de un derecho a la protección contra las injerencias arbitrarias a la vida privada;¹⁶ el Pacto Internacional de Derechos Civiles y Políticos, prevé que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada;¹⁷ la Declaración Universal de Derechos Humanos, establece que nadie será objeto de injerencias arbitrarias en su vida privada;¹⁸ la Declaración Americana de los Derechos y Deberes del Hombre, indica que todas las personas tienen derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.¹⁹

158. En ese sentido, cuando se trate de proteger el derecho a la privacidad, el Estado debe cumplir y hacer cumplir de manera estricta las obligaciones nacionales e internacionales en la materia, en el entendido de que el ámbito a la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas y arbitrarias por parte de terceros, e incluso, de la propia autoridad.

159. A pesar de ello, también es cierto que el derecho a la privacidad no es un derecho absoluto, sino que puede ser objeto de limitaciones restrictivas en su ejercicio, en este caso, cuando surja la necesidad de proteger otros derechos o intereses legítimos, por ejemplo, cuando el interés general pueda verse comprometido o se pudiera perjudicar la convivencia pacífica, incluso, cuando se amenace el orden

¹⁵ Dicho precepto constitucional establece lo siguiente:

Artículo 1o. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.

Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia.

Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley.

Está prohibida la esclavitud en los Estados Unidos Mexicanos. Los esclavos del extranjero que entren al territorio nacional alcanzarán, por este solo hecho, su libertad y la protección de las leyes.

Queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.

¹⁶ El artículo 11.2 de la Convención Americana sobre Derechos Humanos, establece lo siguiente:

Artículo 11. Protección de la Honra y de la Dignidad

[...]

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

¹⁷ El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, establece lo siguiente:

Artículo 17.

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

¹⁸ Declaración Universal de Derechos Humanos.

Artículo 12.

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

¹⁹ El artículo V de la Declaración Americana de los Derechos y Deberes del Hombre establece lo siguiente:

Artículo V. Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

social. Sin que esto implique el desconocimiento del núcleo esencial de tal derecho. En estos supuestos, cierta información concebida como privada, como puede ser el caso de datos personales, puede ser objeto de tratamiento sin que ello signifique que una intromisión injustificada.

160. Entonces, podemos afirmar que el ejercicio del derecho humano a la vida privada podrá ser restringido por el Estado cuando el interés general pudiera ser comprometido, pueda perjudicarse la convivencia pacífica o exista una cuestión de orden público e interés social, siempre que dicha injerencia tenga un sustento constitucional y no sea desmedida o arbitraria.
161. En el caso, tenemos que existe una cuestión de interés general que pudiere perjudicar la convivencia pacífica y que resulta de orden público e interés social, consistente en el combate al lavado de activos, el financiamiento al terrorismo, a la proliferación de armas de destrucción masiva y, en general, la protección del sistema financiero en su conjunto. De este modo, se observa un asidero constitucional en términos de lo previsto en los artículos 21 y 25, segundo párrafo, de la CPEUM.
162. Igualmente, no se observa que la injerencia sea desmedida o arbitraria, ya que la geolocalización otorga un mayor control sobre el uso de dispositivos y facilita la identificación de sus portadores, así como ubicar las zonas de mayor riesgo en la comisión de los ilícitos antes mencionados. Es una medida idónea y eficaz para procurar la seguridad de las operaciones financieras que se lleven a cabo a distancia por medio de dispositivos electrónicos.
163. Es una herramienta que genera, de manera inmediata y precisa, legitimidad en las transacciones, reducción potencial del error humano, facilidad de identificación y notificación de transacciones sospechosas, también, permite identificar el comportamiento del cliente como base para determinar cuándo sus operaciones financieras parecen inusuales. Tiene beneficios para el usuario del sistema financiero, ya que se puede corroborar la validez de una transacción y optimizar la seguridad de los datos, lo cual, reduce los fraudes y el robo de identidad, al generar un historial de transacciones.
164. Sumado a esto, no implica que la institución financiera conozca en todo momento la ubicación de sus clientes, sino que únicamente identifica las coordenadas de latitud y longitud en donde se realiza alguna transacción u operación financiera. Esto es, no existe una geolocalización en sí misma del cliente, sino del dispositivo electrónico en el que se lleva a cabo la operación y únicamente respecto del lugar en donde realiza ésta. Incluso, por los términos en que se encuentra establecida, no implica que tal norma se encuentre dirigida hacia los dispositivos electrónicos personales de comunicación de los clientes, pues la operación puede realizarse desde cualquier dispositivo con acceso a internet, como puede ser una desktop, una laptop, un iPad o tableta, por nombrar algunos.
165. Tampoco debe pasar inadvertido que la geolocalización prevista para el caso de operaciones financieras no presenciales realizadas a través de dispositivos electrónicos, se encuentra sujeta a la voluntad del propio usuario, en tanto que es él quien decide el lugar, momento y dispositivo en donde éstas se llevan a cabo, o bien, puede determinar realizar sus operaciones financieras de manera presencial, directamente en las sucursales habilitadas para tal efecto por la institución financiera de que se trate.

166. Por tanto, las disposiciones 4 Ter, primer párrafo y fracción VII, 16 Bis, párrafos segundo y tercero, 24, párrafo segundo, 25 Bis, párrafo cuarto, de la Resolución que reforma, adiciona y deroga diversas de las disposiciones de carácter general a que se refiere el artículo 115 de la LIC, publicada en el DOF el veintidós de marzo del dos mil diecinueve, son acordes al orden constitucional.

167. En las relatadas circunstancias, ante lo **infundado** de los argumentos de la quejosa, lo que se impone es **negar el amparo** contra las disposiciones en comento.

168. La negativa se hace extensiva a la resolución de veintidós de febrero del dos mil veintitrés dictada por el Pleno del INAI en el expediente *********, debido a que su reclamo lo dirige a la aplicación de las obligaciones contenidas en los artículos y disposiciones que se declararon constitucionales en los párrafos que anteceden.
169. No pasa inadvertido el hecho de que recurrente aduce que las normas reclamadas no superan el test de proporcionalidad porque, si bien, pueden tener un fin constitucionalmente válido como es la prevención y persecución de delitos, lo objetivamente cierto es que no existe prueba demostrativa de que la geolocalización sirva para cumplir dichos fines y porque el grado de afectación que provocan es mucho mayor que el grado de satisfacción del fin perseguido.
170. Con todo, esta Sala estima que dicho argumento deviene **inoperante** toda vez que, si bien, es cierto existen diversos métodos o herramientas argumentativas para que se analice si existen o no las violaciones que aleguen las partes respecto a alguna norma, también lo es que esos métodos no constituyen, por sí mismos, un derecho fundamental, sino la vía para que los jueces cumplan la obligación que tienen a su cargo, que se constriñe a decidir, en cada caso particular, si ha existido o no la violación alegada.
171. En ese sentido, esta Sala no está obligada a verificar la violación a un derecho humano a la luz de un método en particular, ni siquiera porque así se lo hubieran propuesto en la demanda o en el recurso, máxime que no existe exigencia constitucional, ni siquiera jurisprudencial, para emprender el test de proporcionalidad o alguno de los otros métodos cuando se alegue violación a un derecho humano.
172. Sirve de apoyo la jurisprudencia 2a./J. 10/2019 (10a.), de rubro: **“TEST DE PROPORCIONALIDAD. AL IGUAL QUE LA INTERPRETACIÓN CONFORME Y EL ESCRUTINIO JUDICIAL, CONSTITUYE TAN SÓLO UNA HERRAMIENTA INTERPRETATIVA Y ARGUMENTATIVA MÁS QUE EL JUZGADOR PUEDE EMPLEAR PARA VERIFICAR LA EXISTENCIA DE LIMITACIONES, RESTRICCIONES O VIOLACIONES A UN DERECHO FUNDAMENTAL”**.²⁰
173. Tampoco pasa inadvertido el hecho de que la recurrente señala que la normatividad reclamada restringe el libre ejercicio de la libertad de expresión, no obstante, se trata de afirmaciones sin respaldo, ya que no exponen de manera razonada por qué consideran que los actos que impugnan son inconstitucionales o ilegales, respecto al libre ejercicio de la libertad de expresión y esta Segunda Sala tampoco advierte

²⁰ Datos de localización: Semanario Judicial de la Federación y Gaceta, Novena Época, Pleno de la Suprema Corte de Justicia de la Nación, Libro 63, febrero de 2019, Tomo I, página 838, número de registro: 2019276.

violación o restricción alguna al efecto. En ese sentido, dicho argumento resulta **inoperante**.

174. Finalmente, no es obstáculo el hecho de que no se haya realizado el emplazamiento de las Cámaras del Congreso de la Unión y al Presidente de la República que emitieron las aludidas disposiciones legales, pues en la presente resolución se declara la constitucionalidad de las normas en materia, por lo que resulta innecesario reponer el procedimiento para llamarlas a juicio a fin de que, en su caso, defiendan la constitucionalidad de estas.

VI. REVISIÓN ADHESIVA

175. En atención a la conclusión alcanzada, procede declarar **sin materia** la revisión adhesiva interpuesta por el Director de Amparos Contra Leyes, en suplencia por ausencia de la Subprocuradora Fiscal Federal de Amparos, en representación de la SHCP, dado que, por su naturaleza accesoria, al haberse negado la sentencia recurrida, a nada práctico conduciría analizar lo esgrimido por el recurrente adhesivo. En ese sentido se ha pronunciado esta Segunda Sala de esta SCJN en la tesis 2a./J. 166/2007, de los siguientes rubro y texto:

“REVISIÓN ADHESIVA EN AMPARO INDIRECTO. DEBE DECLARARSE SIN MATERIA SI LA REVISIÓN PRINCIPAL RESULTA INFUNDADA.” El artículo 83, fracción IV, de la Ley de Amparo prevé la procedencia del recurso de revisión contra las sentencias pronunciadas por los Jueces de Distrito, y en su último párrafo establece que en todos los casos a que se refiere ese precepto, la parte que obtuvo resolución favorable a sus intereses puede adherirse a la revisión principal. Ahora bien, si se toma en cuenta que el recurso de revisión adhesiva carece de autonomía, al señalar el párrafo indicado que la adhesión al recurso sigue la suerte procesal de éste, es evidente que si la revisión principal resulta infundada, aquél debe declararse sin materia, por su naturaleza accesoria.²¹

176. Por otra parte, resulta aplicable por analogía lo pronunciado por la Primera Sala de esta SCJN, en la tesis 1a./J. 70/99, de los siguientes rubro y texto:

“REVISIÓN ADHESIVA. IMPROCEDENTE.” Si el recurso de revisión principal se declara improcedente, la adhesiva debe seguir la misma suerte procesal de aquél, con fundamento en lo dispuesto por el artículo 83, fracción V, último párrafo de la Ley de Amparo, máxime que en ese supuesto no habrá razón alguna para que la revisión adhesiva sea sustanciada y porque la posibilidad de que sea revocada o modificada habrá desaparecido.²²

VII. DECISIÓN

Por lo antes expuesto y fundado, la Segunda Sala de esta Suprema Corte de Justicia de la Nación, resuelve:

PRIMERO. En la materia del recurso, se **MODIFICA** la sentencia recurrida.

SEGUNDO. Se **SOBRESEE** en el juicio respecto de la disposición tercera transitoria, fracción V, de la Resolución que reforma, adiciona y deroga diversas de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito, publicada en el Diario Oficial de la Federación el veintidós de marzo del dos mil diecinueve.

²¹ Registro digital: 171304, Tesis: 2a./J. 166/2007, Semanario Judicial de la Federación y su Gaceta. Tomo XXVI, septiembre de 2007, página 552.

²² Registro digital: 192997 Tesis: 1a./J. 70/99, Semanario Judicial de la Federación y su Gaceta. Tomo X, noviembre de 1999, página 383.

TERCERO. La Justicia de la Unión **NO AMPARA NI PROTEGE** a *****
contra los artículos 25 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 105 y 107 de su reglamento y las disposiciones 4 Ter, primer párrafo y fracción VII, 16 Bis, párrafos segundo y tercero, 24, párrafo segundo, 25 Bis, párrafo cuarto, de la Resolución que reforma, adiciona y deroga diversas de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito, publicada en el Diario Oficial de la Federación el veintidós de marzo del dos mil diecinueve, en materia de geolocalización, así como contra la resolución de veintidós de febrero del dos mil veintitrés dictada por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el expediente *****.

CUARTO. Queda **SIN MATERIA** la revisión adhesiva.

Notifíquese con testimonio de esta ejecutoria. En su oportunidad, archívese el toca como asunto concluido.