

**RECURSOS DE RECLAMACIÓN 56/2021-CA Y 57/2021-CA
DERIVADOS DE LA ACCIÓN DE INCONSTITUCIONALIDAD
82/2021 Y SU ACUMULADA 86/2021**

Asunto: Se presenta escrito en calidad de *Amicus Curiae*

H. SEGUNDA SALA DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN.

P R E S E N T E

LUIS FERNANDO GARCÍA MUÑOZ, Director de la organización sin fines de lucro **RED EN DEFENSA DE LOS DERECHOS DIGITALES** (en adelante “R3D”), con el debido respeto comparezco por medio del presente escrito ante esta Suprema Corte de Justicia de la Nación (en adelante “SCJN”), en calidad de **AMICUS CURIAE**, para exponer consideraciones de derecho con el objeto de contribuir a la resolución de los Recursos de Reclamación 56/2021-CA y 57/2021-CA promovidos por diversos Senadores de la República, integrantes de la LXIV Legislatura y por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales respectivamente, en contra del proveído de 27 de mayo de 2021, dictado por la Ministra Instructora Norma Lucía Piña Hernández, en la Acción de Inconstitucionalidad 82/2021 y su acumulado 86/2021, en el que se negó la suspensión respecto de la norma general impugnada.

I. INTERÉS DEL PROMOVENTE

La RED EN DEFENSA DE LOS DERECHOS DIGITALES (R3D)¹ es una organización sin fines de lucro dedicada a la defensa de los derechos humanos en el entorno digital. R3D utiliza diversas herramientas legales y de comunicación para hacer investigación de políticas, litigio estratégico, incidencia pública y campañas con el objetivo de promover los derechos digitales en México; incluyendo los derechos a la privacidad, al acceso a las tecnologías de la información y la comunicación, a la libertad de expresión, entre otros.

¹ www.r3d.mx

En este sentido, para R3D la resolución del presente recurso de reclamación, así como la acción de inconstitucionalidad de la cual se deriva el recurso, puede impactar de manera significativa los derechos humanos de la sociedad. En particular, consideramos que de no concederse la suspensión respecto de los efectos y consecuencias del decreto que crea en Padron Nacional de Usuarios de Telefonía Móvil (PANAUT), se materializarían de manera inminente violaciones a los derechos humanos como los derechos a la privacidad, a la protección de datos personales, al acceso a las tecnologías de la información y la comunicación y el derecho de acceso a la justicia, entre otros.

Por ello, a continuación presentamos consideraciones de derecho tendientes a demostrar la procedencia de la suspensión respecto de los efectos y consecuencias de las normas generales impugnadas, las cuales amenazan de manera inminente los derechos humanos de la sociedad mexicana.

II. PARA LA PROCEDENCIA DE LA SUSPENSIÓN DE NORMAS GENERALES EN LA ACCIÓN DE INCONSTITUCIONALIDAD NO SE REQUIERE QUE LOS EFECTOS VIOLATORIOS SE GENEREN DE FORMA INMEDIATA A PARTIR DE LA ENTRADA EN VIGOR DEL DECRETO, SINO QUE BASTA QUE LOS ACTOS VIOLATORIOS SEAN DETERMINADOS, INCLUYENDO LOS ACTOS FUTUROS DE REALIZACIÓN INMINENTE.

Como ha sido señalado en diversas ocasiones por la SCJN, incluyendo por esta Segunda Sala², a partir de una interpretación integral de los artículos 1o Constitucional y 64 de la Ley Reglamentaria de las fracciones I y II de la Constitución Política de los Estados Unidos (en adelante “Ley Reglamentaria”) es factible conceder la suspensión respecto de normas generales en la acción de inconstitucionalidad “en aquellos casos en que la controversia se hubiera planteado

² Ver por ejemplo: Recurso de Reclamación 91/2018-CA, Derivado del incidente de suspensión de la Acción de Inconstitucionalidad 105/2018 y su acumulada 108/2018. Sentencia del 13 de Febrero de 2019.

respecto de normas generales que impliquen o puedan implicar la transgresión irreversible de algún derecho humano”.

Lo cual tiene como fin, en primer lugar, “**preservar la materia del juicio**, asegurando provisionalmente el bien jurídico de que se trate para que la sentencia que, en su caso, declare el derecho de la parte actora, pueda ejecutarse eficaz e íntegramente” y, en segundo lugar, tiene como objetivo “**prevenir el daño trascendente que pudiera ocasionarse a las partes y a la sociedad en general**, en tanto se resuelve el juicio principal, vinculando a las autoridades contra las que se concede a cumplirla, en aras de proteger el bien jurídico de que se trate y sujetándolas a un régimen de responsabilidades cuando no la acaten”.

Si bien en el acuerdo recurrido se reconoce la posibilidad del otorgamiento de la medida cautelar respecto de los efectos y consecuencias de normas generales en la acción de inconstitucionalidad, la Ministra Instructora añade el requisito de que dichos efectos “se recientan [SIC] de manera inmediata a partir de la expedición del decreto cuya invalidez se solicita”.

Al respecto, esta Segunda Sala debe, en primer término, rechazar que para el otorgamiento de la medida suspensiva se requiera la “inmediatez” de los efectos violatorios a partir de la entrada en vigor del decreto impugnado, pues únicamente basta acreditar que los actos potencialmente violatorios sean “determinados”, es decir, que aún siendo actos futuros, los mismos sean de realización inminente.

En efecto, esta Segunda Sala ha acudido en múltiples ocasiones, como en el Recurso de Reclamación 28/2016-CA o el Recurso de Reclamación 46/2020-CA, a criterios que determinan lo que debe entenderse por un acto futuro incierto y su diferencia con los actos futuros de realización inminente. A saber:

“ACTOS FUTUROS, NO LO SON LOS INMINENTES. Son futuros aquellos actos en que sea remota la ejecución de los hechos que se previenen, pues de otro modo se estimarían como no futuros sólo los que ya se han ejecutado. No pueden simplemente considerarse actos futuros aquellos en los que existe la inminencia de la ejecución del acto, desde luego, o mediante determinadas condiciones.”

“ACTOS FUTUROS, CERTEZA DE LOS, EN CASO DE NO CUMPLIRSE DETERMINADA OBLIGACIÓN. Cuando se tiene la certidumbre de que un acto se ejecutará de no cumplirse determinado mandato de la autoridad que lo condiciona, cabe en contra de dicho acto la defensa constitucional, por no constituir un acto futuro o incierto, sino el que es consecuencia cierta, concreta y determinada, del cumplimiento de una obligación.”

A partir de estos criterios, la Segunda Sala de esta SCJN ha entendido que, por un lado, existen actos futuros e inciertos y, por el otro, actos futuros pero inminentes; en los primeros su realización está sujeta a meras eventualidades que pueden o no acontecer; en los segundos prevalece la certeza de que se realizarán, ya sea de inmediato o cumplidas ciertas condiciones.

En este sentido, debe apreciarse que a partir del Decreto impugnado, se suscitan una serie de actos respecto de los cuales es evidente que se está frente a actos futuros de realización inminente como se desglosa a continuación.

1. La obligación de emitir disposiciones administrativas de carácter general por parte del IFT.

De conformidad con lo que señala el artículo segundo transitorio del decreto impugnado, el IFT cuenta con 180 días para la emisión de disposiciones administrativas de carácter general. De esta manera, existe certeza de que en ausencia de una medida suspensiva es inminente la realización de este acto.

Inclusive, el decreto dispone que la no emisión de las disposiciones en el plazo señalado dará lugar a responsabilidades administrativas. Por ende no existe duda respecto de su naturaleza como acto de realización inminente.

2. La cancelación de líneas telefónicas sin derecho a reactivación respecto de personas usuarias que hayan adquirido las líneas telefónicas con anterioridad al decreto.

El artículo cuarto transitorio del decreto impugnado dispone un plazo de dos años, contados a partir de la entrada en vigor del decreto para que las personas usuarias que hayan adquirido líneas telefónicas con anterioridad a la entrada en vigor decreto entreguen datos personales, incluyendo datos personales sensibles como los datos biométricos. Transcurrido el plazo señalado el IFT solicitará a los concesionarios de telecomunicaciones y, en su caso, a los autorizados, “la cancelación en forma inmediata” de las líneas de telefonía móvil, sin derecho a reactivación, que no hayan sido identificadas o registradas por las personas usuarias o clientes.

De nuevo, es claro que el acto de cancelación de líneas telefónicas no es un acto futuro incierto, sino que se trata de un acto futuro de realización inminente, en tanto dicho plazo de dos años comenzó a transcurrir a partir del día siguiente de la publicación del decreto en el Diario Oficial de la Federación, lo cual ocurrió el 16 de abril del presente año. Por lo tanto, de no concederse la suspensión será inminente e ineludible el agotamiento del plazo, generando así sus efectos y consecuencias potencialmente violatorias.

Es importante reiterar que el transcurso de este plazo no está condicionado a acto alguno, ni siquiera a la emisión de las disposiciones administrativas de carácter general que ineludiblemente deben ser emitidas por el IFT. Además debe resaltarse que a la fecha no existe medida suspensiva vigente que haya suspendido el transcurso de dicho plazo, por lo ante la ausencia de la suspensión dicho plazo continúa transcurriendo.

3. El condicionamiento del acceso a la telefonía móvil a la entrega de datos personales, incluyendo datos personales sensibles como los datos biométricos respecto de nuevos usuarios.

Finalmente, el artículo transitorio quinto del decreto impugnado establece que los concesionarios de telecomunicaciones y, en su caso, los autorizados, deberán condicionar el acceso a la telefonía móvil por parte de nuevas personas usuarias a la entrega de datos personales, incluyendo datos personales sensibles como los datos biométricos, transcurrido un plazo de seis meses contados a partir de que el IFT emita las disposiciones administrativas de carácter general.

Dado que ante la ausencia de una medida suspensiva la emisión de dichas disposiciones es inminente, lo es también el establecimiento de la condicionante referida para el ejercicio del derecho de acceso a las tecnologías de la información y la comunicación a través de la telefonía móvil.

De esta manera, de nuevo nos encontramos ante actos futuros pero de realización inminente respecto de los cuales, como ha sido fundamentado resulta posible conceder la suspensión para preservar la materia del juicio o para evitar daños trascendentes e irreversibles a los derechos humanos de millones de personas usuarias de telefonía móvil y de la sociedad en general, como será justificado en el siguiente apartado.

III. LA SUSPENSIÓN DE LAS NORMAS GENERALES IMPUGNADAS ES NECESARIA PARA PRESERVAR LA MATERIA DEL JUICIO Y PARA EVITAR DAÑOS TRASCENDENTES E IRREVERSIBLES A LOS DERECHOS HUMANOS

Una vez que ha sido demostrado que los efectos y consecuencias emanados del decreto impugnado son de inminente realización, procede acreditar las razones por las cuales es necesario conceder la suspensión para preservar la materia del juicio, así como para evitar daños trascendentes e irreversibles a los derechos humanos.

1. Es necesario suspender la obligación de emitir disposiciones administrativas de carácter general por parte del IFT para preservar la materia del juicio.

Una de las cuestiones que forman parte de la materia del mecanismo de control constitucional, es el análisis respecto de si delegar a una autoridad administrativa la definición de aspectos sustantivos, como la precisión de los datos biométricos que serán recolectados y almacenados de manera obligatoria como parte del PANAUT, es compatible con el parámetro de regularidad constitucional, en particular, sí no se vulnera el principio de reserva de ley, y con ello, el principio de legalidad respecto del derecho a la privacidad y protección de datos personales.

En efecto, las normas impugnadas, en particular los artículos 180 Bis, 180 Ter, fracción VI y el Artículo Tercero transitorio del Decreto por virtud del cual se crea el PANAUT, delegan en una autoridad administrativa, el IFT, la definición de cuestiones atinentes a la sustancia, contenido y alcance del derecho a la protección de datos personales, en particular, la definición de los datos biométricos que serán recolectados y almacenados de manera obligatoria.

De esta manera, las interferencias e intromisiones en la vida privada y en la protección de datos personales que las normas impugnadas provocan, pretenden ser definidas en su sustancia, contenido y alcance en una norma reglamentaria y no en una ley formal y material como la Constitución y las normas de derechos humanos de fuente internacional requieren.

Para apreciar la apariencia del buen derecho, es pertinente hacer referencia a la Jurisprudencia P./J. 30/2007 **FACULTAD REGLAMENTARIA. SUS LÍMITES**³ en la cual se establece que “la facultad reglamentaria está limitada por el principio de reserva de ley, el cual se presenta “cuando una norma constitucional reserva

³ Semanario Judicial de la Federación y su Gaceta. “ FACULTAD REGLAMENTARIA. SUS LÍMITES” Tesis Jurisprudencial P./J. 30/2007 Tomo XXV, Mayo de 2007, página 1515 Registro: 172521 Tipo: Jurisprudencia.

expresamente a la ley la regulación de una determinada materia, por lo que excluye la posibilidad de que los aspectos de esa reserva sean regulados por disposiciones de naturaleza distinta a la ley, esto es, por un lado, el legislador ordinario ha de establecer por sí mismo la regulación de la materia determinada y, por el otro, la materia reservada no puede regularse por otras normas secundarias, en especial el reglamento”.

Así, la CPEUM establece de manera reiterada y explícita que las restricciones al derecho a la protección de datos personales deben establecerse en ley, como a continuación se demuestra:

- Artículo 6°, apartado A, fracción II: 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**.
- Artículo 6°, apartado A, fracción II: La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados **en los términos que establezca la ley**.
- Artículo 16, párrafo segundo: Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, **en los términos que fije la ley**.

En este sentido, el artículo 30 de la Convención Americana sobre Derechos Humanos, el cual forma parte del parámetro de regularidad constitucional⁴ establece que “las restricciones permitidas [...] al goce y ejercicio de los derechos y libertades [...] no pueden ser aplicadas sino conforme a leyes que se dicten por razones de interés general y con el propósito para el cual han sido establecidas”.

⁴ Semanario Judicial de la Federación. “Parámetro de la Regularidad Constitucional, Se Extiende a la Interpretación De la Interpretación de la Norma Nacional o Internacional” Libro 24, Noviembre de 2015, Tomo I , página 986 Tesis aislada: 1a. CCCXLIV/2015 (10a.) Registro: 2010426

Al respecto, la Corte Interamericana de Derechos Humanos (en adelante “Corte IDH”) en su jurisprudencia reiterada y desde la emisión de la **Opinión Consultiva OC-6/86**⁵, ha establecido contundentemente que “la expresión leyes, en el marco de la protección a los derechos humanos, carecería de sentido si con ella no se aludiera a la idea de que la sola determinación del poder público no basta para restringir tales derechos. Lo contrario equivaldría a reconocer una virtualidad absoluta a los poderes de los gobernantes frente a los gobernados. En cambio, el vocablo leyes cobra todo su sentido lógico e histórico si se le considera como una exigencia de la necesaria limitación a la interferencia del poder público en la esfera de los derechos y libertades de la persona humana. La Corte [IDH] concluye que la expresión leyes, utilizada por el artículo 30, no puede tener otro sentido que el de ley formal, es decir, norma jurídica adoptada por el órgano legislativo y promulgada por el Poder Ejecutivo, según el procedimiento requerido por el derecho interno de cada Estado.”

En consonancia con lo anterior, como fue señalado anteriormente, la Segunda Sala de la SCJN ha reconocido, al resolver por unanimidad el **Amparo en Revisión 888/2017**⁶ que respecto al derecho a la privacidad y a la protección de datos personales debe respetarse el principio de reserva de ley, por lo que no pueden delegarse facultades legislativas a favor de una autoridad administrativa cuestiones atinentes a la sustancia, contenido y alcance del derecho a la protección de datos personales.

De esta manera es claro que las normas impugnadas, en especial el artículo 180 Ter, fracción VI de la LFTR, al delegar en el IFT la definición de los datos biométricos que serán recolectados y almacenados obligatoriamente respecto de todas las personas que ejercen su derecho de acceso a la telefonía móvil, están delegando en una autoridad administrativa cuestiones atinentes a la sustancia,

⁵ Corte IDH. Opinión Consultiva OC-6/86 “LA EXPRESIÓN LEYES EN EL ARTÍCULO 30 DE LA CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS” 9 DE mayo DE 1986 https://www.corteidh.or.cr/docs/opiniones/seriea_06_esp.pdf -

⁶ SCJN. Amparo Directo en Revisión 888/2017. Resuelto por la Segunda Sala con unanimidad de votos en sesión del 07 de junio de 2017. Ponente: Alberto Perez Dayán. De este precedente derivó la Tesis 2a. CXLI/2017 (10a.) con rubro: “PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES . EL ARTÍCULO 60. PÁRRAFO ÚLTIMO DE LA LEY FEDERAL RELATIVA, NO VULNERA EL PRINCIPIO DE RESERVA DE LEY”. Registro: 2015161

contenido y alcance del derecho a la protección de datos personales, incumpliendo así el parámetro de regularidad constitucional, actualizándose así una violación al principio de legalidad y al principio de reserva de ley que deriva en la apariencia de inconstitucionalidad de las normas combatidas.

Con independencia de la apariencia del buen derecho que se considera existe en el presente caso, es claro que de no concederse la suspensión para evitar transcurra el plazo dado al IFT para la emisión de las disposiciones administrativas de carácter general, se estaría materializando una posible violación al principio de reserva de ley, a la legalidad y a la seguridad jurídica, en conexión con los derechos a la privacidad y protección de datos personales, dejando sin materia, al menos de manera parcial, al medio de control constitucional.

Por lo tanto, se considera que resulta procedente conceder la suspensión para el efecto de interrumpir el plazo fijado al IFT para la emisión de las disposiciones administrativas de carácter general, de manera que la SCJN continúe estando en posibilidad de analizar si dicha delegación de facultades resulta ser compatible con el parámetro de regularidad constitucional.

2. *Es necesario conceder la suspensión para evitar la cancelación, sin derecho a reactivación, de líneas telefónicas adquiridas con anterioridad a la entrada en vigor del decreto, lo cual puede producir afectaciones irreversibles al derecho a la privacidad y a la protección de datos personales, así como daños trascendentes en el acceso a las tecnologías de la información y la comunicación, así al ejercicio de múltiples derechos dependientes de dicho acceso.*

El decreto que contiene las normas impugnadas condiciona el acceso al servicio de telefonía móvil al tratamiento obligatorio de datos personales, incluyendo datos personales sensibles, al establecer en el artículo 180 Quáter que “el registro del número de una línea telefónica móvil en el Padrón Nacional de Usuarios de

Telefonía Móvil será obligatorio para el usuario”. Inclusive, se desprende los artículos 190, fracción VII y el artículo cuarto transitorio que la omisión de acudir ante el concesionario o autorizado para la entrega de la información y los datos personales que dispone el artículo 180 Ter, sería motivo cancelación de la prestación del servicio relacionado con la línea telefónica móvil de que se trate, sin derecho a reactivación.

En este sentido, se considera que, de no concederse la suspensión de los efectos y consecuencias del decreto impugnado, podrían materializarse violaciones al derecho de acceso a las TIC reconocido en el artículo 6 de la CPEUM, 13 de la CADH y 19 del PIDCP, que podrían afectar severamente el ejercicio de otros derechos humanos.

Como desarrolla la CPEUM, el derecho de acceso a las TIC conlleva la obligación estatal de garantizar “el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet”. Igualmente, en la fracción II del apartado B del artículo 6o constitucional, se detalla que “[l]as telecomunicaciones son servicios públicos de interés general, por lo que el Estado garantizará que sean prestados en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre y sin injerencias arbitrarias.”

Como organismos internacionales de derechos humanos han resaltado, el acceso a internet constituye una condición *sine qua non* para el ejercicio efectivo de los derechos humanos hoy en día, incluyendo especialmente los derechos a la libertad de expresión y opinión, asociación y reunión, educación, salud y cultura, entre otros⁷. De esta forma, al ser inseparable del ejercicio pleno de determinados derechos, la CIDH ha considerado que “el acceso a internet debe garantizarse universalmente,

⁷ Relator Especial de las Naciones Unidas (ONU) sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (OEA), y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). *Declaración conjunta sobre libertad de expresión e Internet*. 1 de junio de 2011.

adoptando medidas para cerrar la brecha digital, promoviendo políticas de desarrollo de infraestructura, y protegiendo en todo momento la calidad e integridad del servicio, estableciendo prohibiciones explícitas en torno a bloqueos arbitrarios, parciales o totales y ralentizaciones”⁸.

La falta de acceso a internet incrementa la vulnerabilidad y profundiza la desigualdad, perpetuando la exclusión, por lo que de no asegurarse el acceso de la totalidad de la ciudadanía a los servicios digitales, las comunidades pobres, aisladas y remotas pueden verse doblemente perjudicadas al perder el acceso a la totalidad de los servicios de comunicación, y no solo a los digitales⁹.

En atención de lo anterior, se ha entendido que el Estado posee diversas obligaciones positivas y negativas respecto derecho de acceso a las TIC, dentro de las cuales se encuentra el deber de tomar acciones para promover, progresivamente, el acceso universal a internet -entendido no solo como el acceso a la infraestructura, sino también a la tecnología necesaria para su uso y a la mayor cantidad posible de información disponible en la red-; eliminar las barreras arbitrarias de acceso a la infraestructura, la tecnología y la información en línea; y adoptar medidas de diferenciación positiva para permitir el goce efectivo de este derecho a personas o comunidades que así lo requieran por sus circunstancias de marginación o discriminación¹⁰.

Igualmente se ha resaltado que el acceso universal a internet requiere que el Estado garantice la calidad e integridad del servicio de internet protegiéndolo en todos los casos de bloqueos, interferencias o ralentizaciones arbitrarias. La interrupción del acceso a internet aplicada a poblaciones enteras o a segmentos de la población nunca está justificada, ni siquiera por razones de seguridad nacional¹¹.

⁸ CIDH. *Estándares para una Internet libre, abierta e incluyente*. OEA/Ser.L/V/II. CIDH/RELE/INF.17/17, 15 de marzo de 2017, párr. 32.

⁹ *Ibidem*, párr. 33; y ONU. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión Frank La Rue*. 16 de mayo de 2011 . A/HRC/17/27.

¹⁰ CIDH. *Libertad de expresión e Internet*, Relatoría Especial para la Libertad de Expresión. OEA/Ser.L/V/II. CIDH/RELE/INF.11/13, 31 de diciembre de 2013, párr. 15; y *Declaración conjunta sobre libertad de expresión e Internet*.

¹¹ CIDH. *Estándares para una Internet libre, abierta e incluyente*. OEA/Ser.L/V/II. CIDH/RELE/INF.17/17, 15 de marzo de 2017, párr. 32.

A la luz de estas consideraciones y de las obligaciones generales de progresividad y no discriminación, es que debe entenderse que el Estado se encuentra obligado a no adoptar medidas que obstaculicen de manera arbitraria el acceso a las TIC, especialmente cuando ello puede tener un efecto discriminatorio en grupos de personas de por sí excluidas en el acceso a las TIC y a otros derechos humanos, como lo son las personas en situación de pobreza o que habitan comunidades rurales.

Al respecto, debe apreciarse que ante la ausencia de una medida suspensiva, se materializarían efectos que constituyen restricciones absolutas al derecho de acceso a las TIC pues podrían significar la cancelación, sin derecho a reactivación, del acceso servicios de telecomunicaciones móviles, los cuales de manera creciente resultan cruciales para el ejercicio de otros derechos como el trabajo, la educación, la salud, la libertad de expresión, los derechos políticos, entre otros, pudiendo generar así daños irreparables para las personas que vean cancelada su línea de telefonía móvil.

Por lo tanto, se considera que resulta procedente conceder la suspensión para el efecto de suspender el plazo concedido por el decreto para el registro de datos personales, y así evitar que, transcurrido el plazo, se materialice la cancelación, sin derecho a reactivación, de líneas telefónicas adquiridas con anterioridad a la entrada en vigor del decreto, pues de lo contrario podrían producirse afectaciones severas y potencialmente irreversibles a los derechos humanos de millones de personas usuarias de telefonía móvil.

3. Es necesario conceder la suspensión para evitar que personas que pretendan adquirir una línea de telefonía móvil les sea exigida la entrega de datos personales, incluyendo datos personales sensibles como los datos biométricos, lo cual puede producir afectaciones irreversibles al derecho a la privacidad y a la protección de datos personales, así como daños

trascendentes en el acceso a las tecnologías de la información y la comunicación, así como al ejercicio de múltiples derechos dependientes de dicho acceso.

El decreto que contiene las normas impugnadas establece, en términos generales, la obligación del IFT de instalar, operar, regular y mantener un Padrón Nacional de Usuarios de Telefonía Móvil¹² (PANAUT), así como la obligación de concesionarios y autorizados¹³ para prestar servicios de telecomunicaciones de recabar y de las personas usuarias de telefonía móvil de entregar, entre otros, datos personales¹⁴ como:

- Número de línea telefónica móvil;
- Nombre completo o, en su caso, denominación o razón social del usuario;
- Nacionalidad;
- Número de identificación oficial con fotografía o Clave Única de Registro de Población del titular de la línea;
- Datos Biométricos del usuario y, en su caso, del representante legal de la persona moral, conforme a las disposiciones administrativas de carácter general que al efecto emita el Instituto;
- Comprobante de domicilio del usuario;

Ante la ausencia de la medida suspensiva, las normas impugnadas establecen que la negativa por parte de las personas usuarias al tratamiento obligatorio¹⁵ de los datos personales enlistados, misma que incluye datos personales sensibles, produciría como consecuencia la imposibilidad de acceder al servicio de telefonía móvil o incluso la cancelación, sin derecho a reactivación, de dicho servicio.

Adicionalmente, el párrafo tercero del artículo 180 Septimus de la LFTR que se combate establece que autoridades de seguridad, procuración y administración de

¹² Artículo 15, fracción XLII Bis de la LFTR.

¹³ Artículo 180 Quintes.

¹⁴ Artículo 180 Ter de la LFTR.

¹⁵ Artículo 180 Quáter de la LFTR.

justicia podrían acceder a la información contenida en el PANAUT sin establecer salvaguardas como el control judicial.

De esta manera, de no suspenderse los efectos y consecuencias del decreto impugnado, de manera inminente se exigiría a decenas de millones de personas usuarias de telefonía móvil el tratamiento obligatorio de datos personales, incluyendo datos personales sensibles como los datos biométricos, derivado de la instalación, operación, regulación y mantenimiento del PANAUT, lo cual pondría en grave riesgo los derechos a la privacidad y a la protección de datos personales.

Del análisis del decreto se desprenden diversas características del PANAUT que resultan fundamentales para apreciar el alto grado de afectación que provocarían en caso de no concederse la suspensión. En particular debe apreciarse el carácter masivo y centralizado de la base de datos que se pretende crear a partir de las normas combatidas.

En efecto, la base de datos del PANAUT pretende abarcar a la totalidad de las personas usuarias de telefonía móvil, es decir, más de 86.5 millones de personas respecto de las cuales, por cierto, no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con la comisión de delitos. Para efectos de apreciar la apariencia del buen derecho, resulta pertinente recordar los precedentes del TJUE en los casos *Digital Rights Ireland*¹⁶ y *Watson vs Reino Unido*¹⁷ en los que este elemento fue valorado para establecer que la recolección y conservación de información sobre la totalidad de las personas usuarias de servicios de telecomunicaciones no resultaban adecuadas al principio de proporcionalidad.

Igualmente, las normas impugnadas predeterminan el diseño centralizado de la base de datos del PANAUT, es decir, obligan al almacenamiento en una sola base

¹⁶ TJUE. *Digital Rights Ireland vs. Minister of Communications, Marine and Natural Resources y otros*. Casos Conjuntos, C-293/12 y C-594/12, 8 de abril de 2014.

¹⁷ TJUE. *Watson y otros. Vs Secretary of State for the Home Department y otros*. Casos Conjuntos, C-203/15 y C-698/15, 21 de diciembre de 2016.

de datos de un número elevado de datos personales. Las bases de datos centralizadas de gran escala conllevan un mayor riesgo al resultar más atractivas para posibles atacantes, ya que permiten que un solo ataque exitoso redunde en la obtención de un gran número de datos valiosos, algo que comúnmente se conoce como “punto único de falla”.

Las consecuencias de una vulneración del PANAUT serían significativamente graves al incluirse a los datos biométricos como parte de la base de datos. Los datos biométricos se refieren a las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, que permiten o confirman la identificación única de una persona¹⁸. Por ejemplo la huella digital, el rostro (reconocimiento facial), la retina, el iris, la geometría de la mano o de los dedos, la estructura de las venas de la mano, la forma de las orejas, la piel o textura de la superficie dérmica, el ADN, la composición química del olor corporal y el patrón vascular, pulsación cardíaca, entre otros.

Como ha sido advertido por organismos internacionales de protección de derechos humanos, la creación de bases de datos de información biométrica a gran escala suscita graves preocupaciones por sus consecuencias para los derechos humanos. Estos son datos particularmente delicados, ya que, por definición, están indisolublemente vinculados a una persona concreta y a su vida, y pueden ser objeto de vulneraciones graves e incluso irreversibles. Por ejemplo, el robo de la identidad a través de los datos biométricos es muy difícil de reparar y puede afectar gravemente a los derechos de una persona¹⁹.

Igualmente, debe tomarse en cuenta que la característica de obligatoriedad del registro en el PANAUT, que dispone el artículo 180 Quáter de la LFTR, representaría, en caso de no concederse la suspensión, una interferencia severa en

¹⁸ Ver: REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento Europeo). Artículo 4, inciso 14.

¹⁹ Consejo de Derechos Humanos “*El derecho a la privacidad en la era digital*”. informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. A/HRC/39/29 3 de agosto de 2018 <https://undocs.org/es/A/HRC/39/29>

el derecho a la protección de datos personales, en particular a los derechos de oposición y cancelación, así como una limitación grave a los principios de licitud, consentimiento, calidad y proporcionalidad. Dicha interferencia ocurre ya que al ser obligatoria la recolección y almacenamiento permanente de los datos personales, se anula de manera absoluta la posibilidad de ejercer el derecho de oposición y se limita gravemente el ejercicio del derecho de cancelación, en tanto este derecho sólo sería posible ejercerlo si se renuncia a la posibilidad de acceder a la telefonía móvil, lo cual acarrea, como ha sido desarrollado anteriormente, una gama de afectaciones trascendentes al derecho de acceso a las TIC y a otros derechos derivados.

Además de los riesgos de daño irreversible derivados de una vulneración o acceso no autorizado a los datos personales, en particular a los datos biométricos, es preciso resaltar los riesgos derivados del acceso a la información contenida en el PANAUT por parte de autoridades de seguridad y procuración de justicia, las cuales podrán acceder a la información contenida en el PANAUT sin que existan salvaguardas adecuadas y suficientes para prevenir el abuso de este acceso, como puede observarse del artículo 180 Séptimus contenido en el decreto impugnado.

Los riesgos asociados a la posibilidad de que autoridades aprovechen el acceso al PANAUT para fines distintos y contrarios a la protección de la seguridad pública, además de ser altamente probables derivado de la ausencia de salvaguardas, son todavía más graves, dado el contexto de colusión frecuente entre autoridades de seguridad y procuración de justicia y la delincuencia organizada, la cual se encuentra ampliamente documentada. Por ejemplo, la CIDH ha constatado que un “aspecto estructural que permea muchas instituciones de justicia en México [...] es la corrupción así como la protección, colusión e infiltración de la delincuencia organizada en diferentes dependencias”²⁰.

²⁰ CIDH. “*Situación de Derechos Humanos en México*”. OEA/Ser.L/V/II. Doc. 44/15. 31 de diciembre 2015. Consulta en: <https://www.oas.org/es/cidh/informes/pdfs/Mexico2016-es.pdf> pág. 498.

En el mismo sentido, también debe tomarse en cuenta el contexto de abuso de medidas de vigilancia e intervención de comunicaciones privadas por parte de autoridades en México que ha sido documentado²¹ y reconocido por autoridades nacionales y por órganos internacionales de derechos humanos.

Por ejemplo, el caso emblemático de adquisición y uso del *malware* de espionaje *Pegasus*, utilizado en contra de personas defensoras de derechos humanos, periodistas y activistas en México²², respecto del cual diversos organismos internacionales de derechos humanos han manifestado preocupación y han realizado recomendaciones²³ y respecto del cual el INAI determinó, al resolver el procedimiento de verificación identificado con la clave INAI.3S.07.01-007/2018²⁴, que la Procuraduría General de la República (PGR) violó la LGPDPSO con el uso de *Pegasus*, al no cumplir con los deberes de seguridad y el principio de responsabilidad.

De igual manera se han documentado otras irregularidades en la adquisición y uso de herramientas y facultades de vigilancia por parte de autoridades de seguridad y procuración de justicia en México, como el despliegue de estas facultades por autoridades incompetentes²⁵, el uso ilegal y sin cumplir con el requisito de control judicial que el artículo 16 de la Constitución y las leyes exigen²⁶, e incluso la adquisición y uso de tecnologías de vigilancia masiva como “las antenas falsas” de

²¹ Privacy International y R3D: Red en Defensa de los Derechos Digitales. “El derecho a la privacidad en los Estados Unidos Mexicanos: informe de actor interesado. Examen Periódico Universal. 31o periodo de sesiones - México”. Marzo 2018. Consulta en:

https://privacyinternational.org/sites/default/files/2018-05/EPU_El%20Derecho%20a%20la%20Privacidad%20en%20los%20Estados%20Unidos%20Mexicanos.pdf

²²R3D: Red en Defensa de los Derechos Digitales. “Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México”. Junio 2017. Disponible en: <https://r3d.mx/gobiernoespia/>

²³ ONU. México: expertos de la ONU piden investigación independiente e imparcial sobre el uso de spyware contra defensores de DD HH y periodistas. Ginebra. 19 de julio de 2017. Disponible en: <http://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=S> ; Informe conjunto del Relator Especial para la libertad de expresión de la CIDH, Edison Lanza, y el Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye, sobre su misión a México. Junio 2018. A/HRC/35/22/Add.3. Disponible en:

http://www.oas.org/es/cidh/expresion/docs/2018_06_18%20CIDH-UN_FINAL_MX_report_SPA.PDF

²⁴ INAI. Expediente: INAI 3S.07.01-007/2018. Disponible en:

<https://home.inai.org.mx/wp-content/documentos/Resolucionesenmateria/INAI.32.07.01-007-2018.pdf>

²⁵ R3D. “El Estado de la Vigilancia: Fuera de Control” Noviembre 2016. Consulta en:

<https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf>

²⁶R3D. “ PGR adquirió equipo para geolocalizar 255 mil celulares en 2018; se usó para espiar a todos los candidatos: Reporte indigo”. 5 de Junio de 2019. Disponible:

<https://r3d.mx/2019/06/05/pgr-equipo-espionaje-celulares-geomatrix/>

telefonía²⁷ y sistemas que permiten “recopilación en masa de (datos de) todos los usuarios de Internet en un país”²⁸.

En particular, debe considerarse que el acceso a la base de datos del PANAUT en conjunto con el despliegue de tecnologías de vigilancia masiva como las “antenas falsas” de telefonía o de sistemas de geolocalización masiva, que como se ha referido en el párrafo anterior se encuentran siendo desplegadas por autoridades en México, potencian aún más los riesgos de vigilancia autoritaria en contra de la población.

A la luz de todas las consideraciones vertidas en los párrafos precedentes, resulta claro que resulta procedente conceder la suspensión para el efecto de suspender los efectos y consecuencias inminentes del decreto impugnado, en particular, el transcurso del plazo señalado para que el IFT emita las disposiciones administrativas de carácter general y, en consecuencia, el plazo para que los concesionarios, y en su caso los autorizados, comiencen a exigir a cualquier persona que desee adquirir una línea de telefonía móvil el tratamiento de datos personales, incluyendo datos personales sensibles como los datos biométricos, pues de lo contrario podrían materializarse afectaciones de grave intensidad en el derecho a la privacidad y protección de datos personales.

4. *Es necesario conceder la suspensión para que, en caso de que la SCJN considere que el decreto no es inconstitucional, el IFT, los concesionarios de telecomunicaciones, y en su caso, los autorizados, cuenten con el tiempo necesario para hacer una adecuada implementación del PANAUT, incluyendo la adopción de medidas de seguridad que mitiguen los riesgos a la privacidad y a la protección de datos personales.*

²⁷ R3D. “Las #GolondrinasenelAlambre: Torres Falsas de Telefonía Para Recolectar Información de Personas”. 3 de junio de 2020. Consulta en: <https://r3d.mx/2020/06/03/las-golondrinasenelalambre-del-gobierno-federal-torres-falsas-de-telefonía-para-recolectar-información-de-personas/>

²⁸ R3D. “#FiscalíaEspía: La FGR adquirió equipo capaz de espiar ilegalmente a todos los usuarios de internet en México”. 14 de abril de 2021. Consulta en: <https://r3d.mx/2021/04/14/fiscaliaespia-la-fgr-adquirio-equipo-capaz-de-espiar-ilegalmente-a-todos-los-usuarios-de-internet-en-mexico/>

Como ha sido desarrollado, el decreto impugnado establece una serie de plazos para la realización inminente de diversos actos potencialmente violatorios de derechos humanos.

Si bien la Ministra Instructora ha interpretado una supuesta ausencia de urgencia en el otorgamiento de la suspensión, derivada de la errónea apreciación de los actos potencialmente violatorios como “inciertos” a pesar de ser inminentes, como ya se ha demostrado, es fundamental apreciar que los plazos definidos en el decreto impugnado no resultan ser gratuitos o triviales, sino que otorgan al IFT, a los concesionarios de telecomunicaciones y a otros actores, del tiempo suficiente para realizar las inversiones, la planeación, diseño e implementación de los sistemas que serían utilizados para la operación del PANAUT.

En este sentido, el retardo injustificado en conceder la suspensión frente a actos cuya realización es inminente podría producir el resultado de que, si en la SCJN no se obtiene la votación calificada para declarar la constitucionalidad del decreto, los entes públicos y privados encargados de la operación del PANAUT no tengan el tiempo insuficiente para la adecuada planeación e instrumentación técnica del PANAUT, agravando así los riesgos para la seguridad de la información, y con ello agravando los riesgos para los derechos humanos de decenas de millones de personas usuarias de telefonía móvil.

En este sentido, es evidentemente necesario que se conceda la suspensión para permitir que, independientemente del resultado de este medio de control de constitucionalidad, no se ponga en innecesario riesgo los derechos humanos de un amplio sector de la sociedad.

5. Debe concederse la suspensión en atención a que, derivado de las restricciones constitucionales y legales que impiden el otorgamiento de la suspensión respecto de normas, actos y omisiones del IFT dentro del juicio de amparo, las personas no contarían con un recurso adecuado y efectivo para evitar la

materialización irreparable de las afectaciones a sus derechos humanos.

Finalmente, debe añadirse que no puede pasar desapercibida la obligación de la autoridad judicial de garantizar el derecho de acceso a la justicia, de desarrollar las posibilidades del recurso judicial, como señala el artículo 25.2 b) de la Convención Americana sobre Derechos Humanos, así como el principio de interpretación más favorable al que se refiere el párrafo segundo del artículo primero constitucional.

En este sentido, debe valorarse que según el artículo 28, fracción VII de la Constitución, así como el artículo 128 de la Ley de Amparo, las normas generales, actos y omisiones del IFT no pueden suspenderse dentro del juicio de amparo. De esta manera, no conceder la suspensión dentro de este medio de control constitucional podría producir una serie de eventos que resultaría imposible para las personas afectadas evitar mediante a través del juicio de amparo, en tanto dicho recurso no resultaría adecuado y efectivo para preservar la materia del juicio previo a su resolución, corriéndose el riesgo de que las violaciones alegadas se consumen de manera irreparable, vulnerando así el derecho de acceso a la justicia de la sociedad, de manera adicional a los múltiples derechos humanos que el PANAUT vulneraría.

Es por ello que, en atención a las circunstancias especiales del presente caso derivadas de la excepcional restricción a la suspensión dentro del juicio de amparo respecto de actos y normas del IFT, que debe concederse la suspensión en este medio de control constitucional, de los efectos y consecuencias que se realizarán de manera inminente e ineludible ante la ausencia de dicha medida cautelar, pudiendo producir daños irreversibles en los derechos humanos de decenas de millones de personas en México, incluyendo el derecho de acceso a la justicia.

IV. CONCLUSIONES

1. Es procedente el otorgamiento de la suspensión de los efectos y consecuencias de normas generales en la acción de inconstitucionalidad cuando los mismos sean futuros determinados, es decir de realización inminente, con el objetivo de preservar la materia del medio de control y prevenir el daño trascendente que pudiera ocasionarse a los derechos humanos y a la sociedad en general.
2. El decreto impugnado produce efectos y consecuencias de realización inminente como la emisión de disposiciones administrativas de carácter general por parte del IFT, el condicionamiento del acceso a la telefonía móvil a la entrega de datos personales sensibles o la cancelación de líneas telefónicas que no hayan sido registradas en el PANAUT.
3. De no concederse la suspensión, podría afectarse la materia del medio de control de constitucionalidad al consumarse la emisión de disposiciones administrativas de carácter general en posible violación del principio de reserva de ley, en conexión con los derechos a la privacidad y a la protección de datos personales, antes de que esta SCJN pueda pronunciarse al respecto.
4. De no concederse la suspensión, se podrían generar violaciones masivas y trascendentes al derecho de acceso a las tecnologías de la información y la comunicación y a otros derechos humanos derivados de dicho acceso, ante el inminente condicionamiento del ejercicio de ese derecho a la entrega de datos personales sensibles, como los datos biométricos y ante la inminente cancelación de las líneas telefónicas que no sean registradas en el PANAUT.

5. De no concederse la suspensión, se podrían generar violaciones irreversibles y permanentes al derecho a la privacidad y a la protección de datos personales derivadas de las posibles vulneraciones de datos personales, en especial de los datos biométricos, los cuales se encuentran indisolublemente vinculados a una persona concreta, así como del riesgo de abuso en el acceso a los datos personales por parte de autoridades ante la ausencia de salvaguardas adecuadas para prevenir, evitar y remediar instancias de abuso.
6. En caso de que en la resolución del medio de control de constitucionalidad no se determine la declaratoria general de inconstitucionalidad y de no concederse la suspensión, los sujetos obligados a diseñar, implementar el PANAUT podrían no contar con el tiempo necesario para adoptar las medidas de seguridad necesarias para mitigar los riesgos a la seguridad y privacidad de la información que formaría parte del PANAUT, agravándose así los riesgos para la sociedad.
7. En caso de no concederse la suspensión en este medio de control constitucional, las personas podrían quedar en estado de indefensión al no ser posible la suspensión de los actos y normas del IFT, de inminente realización, a través del juicio de amparo, en virtud de las restricciones establecidas en el artículo 28, fracción VII de la Constitución y 128 de la Ley de Amparo, por lo que podría afectarse irreparablemente el derecho de acceso a la justicia en relación a los múltiples derechos humanos se verían afectados de manera inminente a partir del decreto impugnado.

Por lo anteriormente expuesto, a esta H. Segunda Sala de la Suprema Corte de Justicia de la Nación le solicito:

PRIMERO.- Tener por presentado el presente escrito en calidad de *amicus curiae*.

SEGUNDO.- En su oportunidad revoque el auto recurrido y determine la suspensión de los efectos y consecuencias del decreto impugnado.

PROTESTO LO NECESARIO, en la Ciudad de México, a los diecinueve días del mes de agosto del año dos mil veintiuno.

LUIS FERNANDO GARCÍA MUÑOZ

Director de la Red en Defensa de los Derechos Digitales (R3D)