ACCIÓN DE INCONSTITUCIONALIDAD 82/2021 Y SU ACUMULADA 86/2021

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

PLENO 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 formuladas por diversas organizaciones de la sociedad civil con el objeto de contribuir a la resolución de la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021 promovidas 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 (INAI) respectivamente, en contra del "Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión", publicado en el Diario Oficial de la Federación el 16 de abril de 2021, en el que se crea un "Padrón Nacional de Usuarios de Telefonía Móvil" (PANAUT).

I. INTERÉS DE LAS PROMOVENTES

- 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.

- CAMPAÑA GLOBAL POR LA LIBERTAD DE EXPRESIÓN A19, ASOCIACIÓN CIVIL (ARTICLE 19)[2], es una organización independiente y apartidista que promueve y defiende el avance progresivo de los derechos de libertad de expresión y acceso a la

[1] www.r3d.mx
[2] https://articulo19.org/

información de todas las personas, de acuerdo a los más altos estándares internacionales de derechos humanos, contribuyendo así al fortalecimiento de la democracia, incluyendo: La exigencia del derecho a la difusión de información y opiniones en todos los medios; la investigación de amenazas y tendencias; la documentación de violaciones a los derechos de libertad de expresión; el acompañamiento a las personas cuyos derechos han sido violados; y la coadyuvancia en el diseño de políticas públicas en su área de acción.

- OBSERVATEL A.C. es una organización de la sociedad civil, dedicada a realizar estudios e investigaciones, así como elaborar propuestas y opiniones que contribuyan a mejorar las telecomunicaciones, la radiodifusión, los medios de comunicación escrita y electrónica, así como en general las tecnologías de la información y comunicación ("TIC") en México, promover la reducción y eliminación de la brecha digital entendida como la falta de acceso a TIC, fomentar, promover y difundir el derecho de acceso a la información, promover y defender los derechos de los usuarios de las TIC, y apoyar a personas, sectores y regiones de escasos recursos a tener acceso a estos servicios.

- TEDIC, es una organización sin fines de lucro que defiende y promueve los derechos humanos en entornos digitales, con foco en desigualdades de género y sus intersecciones en Paraguay y la región de América Latina. Con la visión hacia una sociedad donde los derechos humanos en espacios digitales sean garantizados para todes. A través de la investigación, difusión de la información y capacitación en temas de privacidad, datos personales, ciberseguridad: cuidados digitales, libertad de expresión y manifestación, neutralidad en la red, derechos de autor, inteligencia artificial, biometría, entre otros con un enfoque transversal de género.

- DERECHOS DIGITALES[3] es una organización no gubernamental independiente y sin fines de lucro, con sede principal en Santiago de Chile y con alcance latinoamericano en su trabajo, que se dedica a la defensa y promoción de los derechos fundamentales en el entorno digital, centrando atención en el impacto sobre estos derechos del uso y la regulación de las tecnologías digitales desde hace más de quince años. Fundada en 2005, Derechos Digitales cuenta con una vasta experiencia en defensa de los derechos humanos en relación al impacto sobre ellos

[3] https://www.derechosdigitales.org/

en el uso de la tecnología. Participa en instancias locales, regionales y globales en que se discuten distintas políticas públicas, acuerdos y regulaciones que conciernen al despliegue de tecnologías a través de las cuales los Estados ejercitan sus funciones, impactando en el ejercicio de los derechos fundamentales de sus ciudadanas.

- La ASOCIACIÓN POR LOS DERECHOS CIVILES (ADC)[4] es una organización de la sociedad civil con sede en Buenos Aires, Argentina que, desde su creación en 1995, trabaja en la defensa y promoción de los derechos civiles y humanos en Argentina y América Latina. La ADC promueve y defiende los derechos fundamentales de las personas, fomenta el fortalecimiento democrático y aboga por una sociedad inclusiva, con especial atención a los grupos en situación de vulnerabilidad, a través de la identificación e investigación de temáticas de vanguardia, el desarrollo de estrategias de incidencia y comunicación, y en particular, el uso del litigio estratégico de interés público.

- El INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR (IDEC) es una asociación civil sin fines de lucro, fundada en 1987, que tiene como objetivo promover la educación, la defensa de los derechos del consumidor y la ética en las relaciones de consumo. Promueve la labor de asistencia social, defensa de los derechos de grupos y minorías y otras formas de desarrollo y defensa de los derechos. Idec es miembro de pleno derecho de Consumers International, federación que agrupa a asociaciones de consumidores de todo el mundo.

- ACCESS NOW[5] es una organización no gubernamental internacional que defiende y extiende los derechos digitales de los usuarios y usuarias en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas globales, el análisis integral de políticas públicas, el financiamiento a grupos locales emergentes, intervenciones jurídicas y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

- HIPERDERECHO[6] es una organización civil sin fines de lucro dedicada a investigar, facilitar el entendimiento público y promover el respeto de los derechos y libertades

[4] https://adc.org.ar
[5] https://www.accessnow.org/
[6] https://hiperderecho.org/

en entornos digitales. Usamos herramientas legales para defender los derechos de todas las personas en entornos digitales y, del mismo modo, buscamos difundir la capacidad liberadora de la tecnología y desarrollar o potenciar espacios digitales para que todos y todas ejerzan sus derechos y refuercen su ciudadanía.

- FUNDACIÓN KARISMA es una organización de la sociedad civil que busca proteger y promover los derechos humanos y la justicia social en el diseño y uso de las tecnologías digitales. Fundada en 2003, KARISMA se posiciona hoy como una de las principales organizaciones de la sociedad civil latinoamericana que trabaja en la promoción de los derechos humanos en el mundo digital.

- FUNDACIÓN INTERNETBOLIVIA.ORG es una organización fundada en 2018 que defiende los derechos humanos en Internet en contra de toda acción que pueda llevar a la censura, vigilancia, manipulación, extorsión, entre otras prácticas nocivas en contra de usuarios y usuarias.

- REDES POR LA DIVERSIDAD, EQUIDAD Y SUSTENTABILIDAD A.C. (REDES AC) es una asociación civil mexicana constituida en 2004 para impulsar la formación de redes de apoyo y facilitación de procesos para organizaciones, grupos y comunidades. Su equipo de trabajo está conformado por personas comprometidas con la diversidad, la equidad y la sustentabilidad. Desde su constitución, trabajan dos áreas principales: Desde nuestra constitución, hemos trabajado en dos áreas principales: Comunicación Indígena y Comunitaria y Desarrollo Comunitario Sustentable.

- PRIVACY INTERNATIONAL es una organización no gubernamental sin fines de lucro que trabaja en la intersección de las tecnologías modernas y los derechos. Fundada en 1990, Privacy International sostiene que la privacidad es esencial para la protección de la autonomía y la dignidad humana, y constituye una base sobre la que se construyen otros derechos humanos. Privacy International investiga cómo se generan y explotan los datos personales de las personas, y cómo pueden protegerse a través de marcos legales y tecnológicos.

En este sentido, para las organizaciones que suscribimos el presente escrito, la resolución de las acciones de inconstitucionalidad pueden impactar de manera significativa los derechos humanos de la sociedad. En particular, consideramos que de no reconocerse la inconstitucionalidad del Decreto que crea el Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT), se materializarán 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 entre otros.

Por ello, a continuación presentamos consideraciones de derecho tendientes a demostrar la incompatibilidad del PANAUT con el parámetro de regularidad constitucional. En particular, los artículos 1, 2 6, 7, 14, 16 y 20 de la Constitución Política de los Estados Unidos Mexicanos (en adelante "CPEUM"), 1.1, 2, 8, 11, 13 y 24 de la Convención Americana sobre Derechos Humanos (en adelante "CADH") y 2, 14.2, 17, 19 y 26 del Pacto Internacional de Derechos Civiles y Políticos (en adelante "PIDCP").

II. CONCEPTOS DE INVALIDEZ

PRIMERO.- EL TRATAMIENTO OBLIGATORIO DE DATOS PERSONALES SENSIBLES PARA LA INSTALACIÓN Y OPERACIÓN DEL PANAUT INTERFIERE CON EL DERECHO A LA PRIVACIDAD Y A LA PROTECCIÓN DE DATOS PERSONALES SIN CUMPLIR CON LOS REQUISITOS DE LEGALIDAD, IDONEIDAD, NECESIDAD Y PROPORCIONALIDAD POR LO QUE VIOLA LOS ARTÍCULOS 6, 14 Y 16 DE LA CPEUM, 11 DE LA CADH Y 17 DEL PIDCP.

El Decreto que contiene las normas combatidas establece, en términos generales, la obligación del Instituto Federal de Telecomunicaciones (en adelante "IFT") de instalar, operar, regular y mantener un Padrón Nacional de Usuarios de Telefonía Móvil[7] (PANAUT), así como la obligación de concesionarios y autorizados[8] para prestar servicios de telecomunicaciones de recabar, y de las personas usuarias de telefonía móvil de entregar, entre otros, datos personales[9] 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;

[7] Artículo 15, fracción XLII Bis de la LFTR.
[8] Artículo 180 Quintes.
[9] Artículo 180 Ter de la LFTR.

- Comprobante de domicilio del usuario;

Las normas combatidas establecen que la negativa por parte de las personas usuarias al tratamiento obligatorio[10] de los datos personales enlistados, misma que incluye datos personales sensibles, produce 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 justicia "podrán acceder a la información" contenida en el PANAUT sin establecer salvaguardas como el control judicial.

De esta manera, esta parte quejosa considera que el tratamiento obligatorio de datos personales, incluyendo datos personales sensibles como los datos biométricos, derivado de la instalación, operación, regulación y mantenimiento del PANAUT vulnera los derechos a la privacidad y a la protección de datos personales como será demostrado a continuación.

Previo al desarrollo de las violaciones específicas, resulta indispensable desarrollar el contenido esencial del derecho a la privacidad y protección de datos personales, de manera que exista claridad respecto del parámetro de regularidad constitucional que debe aplicarse en el presente caso.

A. Contenido del derecho a la privacidad y la protección de datos personales

El derecho a la privacidad y a la protección de datos personales se encuentra reconocido en los artículos 6 y 16 de la CPEUM, así como por diversos instrumentos internacionales de los que México es parte, como el artículo 11 de la CADH y 17 del PIDCP, 16 de la Convención sobre los Derechos de la Niñez y 14 de la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares.

Al interpretar el artículo 11 de la CADH que prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas, la Corte IDH ha interpretado a la vida privada como "un concepto amplio que no es susceptible de definiciones exhaustivas y comprende, entre otros ámbitos protegidos, la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos. Es decir, la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás[11]".

Asimismo, la Corte Interamericana de Derechos Humanos (en adelante "Corte IDH") también ha sostenido que "el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública[12]". Además ha interpretado que "la fluidez informativa que existe hoy en día coloca al derecho a la vida privada de las personas en una situación de mayor riesgo

[10] Artículo 180 Quáter de la LFTR.
[11] Corte IDH. *"Caso Atala Riffo y niñas vs Chile"*. Sentencia de 24 de febrero de 2012. párr. 162.
[12] Corte IDH. "*Caso Tristán Donoso vs Panamá*" Sentencia del 27 de enero de 2009. párr. 55.

debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente. Este progreso (...) no significa que las personas deban quedar en una situación de vulnerabilidad frente al Estado o a los particulares. De allí que el Estado debe asumir un compromiso, aún mayor, con el fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada"[13].

La Suprema Corte de Justicia de la Nación (en adelante "SCJN") también ha destacado recientemente la importancia del derecho a la privacidad, también referido como derecho a la intimidad. En el ***Amparo en Revisión 884/2018***[14], la Primera Sala reconoció por unanimidad que "si bien el derecho a la intimidad suele asociarse con aquello que no pertenece a lo público y a lo que, sólo el individuo, y quienes éste admite libremente, puedan tener acceso, lo cierto es que en el estado de derecho social, el derecho a la intimidad se convierte en el derecho a saber qué, quién y por qué motivos, puede conocer información sobre la persona, pues deja de ser sólo un derecho de defensa de un espacio exclusivo y excluyente, para convertirse también en un derecho activo de control sobre la información personal, de que otros puedan disponer y del uso que se le dé".

Asimismo, la Primera Sala recalca que "las potenciales agresiones que la posesión de la información personal organizada (que obra generalmente en registros informáticos), representan para la intimidad, tienen una relevancia pública enorme, ya que el derecho a la intimidad y el derecho a la información, además de tener un aspecto de protección de bienes individuales, tienen una importante función para el desarrollo de sociedades democráticas porque son, bien entendidas, una condición para el ejercicio del resto de los derechos humanos"[15].

El derecho a la protección de datos personales, por su parte, además de encontrarse reconocido en el artículo 16 de la CPEUM, se encuentra desarrollado, entre otros instrumentos, en el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (en adelante "Convenio 108") publicado en el Diario Oficial de la Federación el 28 de Septiembre de 2018 y en las Leyes de protección de datos personales en posesión de particulares (en adelante "LFPDPPP") y de sujetos obligados (en adelante "LGPDPPSO").

El derecho a la protección de datos personales implica, de manera destacada, la obligación de que cualquier tratamiento[16] de datos personales[17] respete los principios de licitud,

---

[13] Corte IDH. "*Caso Escher y otros vs Brasil*" Sentencia de 6 de julio de 2009. párr. 115.
[14] SCJN. Primera Sala. Amparo en revisión 884/2018. Aprobado por unanimidad de votos en la sesión celebrada el 15 de mayo de 2019. Ponente: Ministra Norma Lucía Piña Hernández.
[15] Ibídem. p. 24.
[16] El artículo 3 fracción XVIII de la LFPDPPP y 3 fracción XXXIII de la LGPDPPSO entienden por tratamiento: "Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales".
[17] El artículo 3 fracción V de la LFPDPPP y 3 fracción IX de la LGPDPPSO entienden por datos personales: "Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información".

consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad[18], e impone obligaciones incluso más estrictas cuando el tratamiento se refiere a datos personales sensibles.

Los datos sensibles son definidos por la LFPDPPP y la LGPDPPSO como “aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual”.

Igualmente, la LGPDPPSO dispone la obligación de realizar una Evaluación de Impacto a la Privacidad (en adelante “EIP”) cuando “se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen el tratamiento intensivo o relevante de datos personales”[19].

Naturalmente, el derecho a la privacidad y a la protección de datos personales no es un derecho absoluto y admite restricciones. Sin embargo, las restricciones al derecho a la privacidad y a la protección de datos personales deben satisfacer estrictos requisitos para poder considerarse acordes al parámetro de regularidad constitucional.

Como la Corte IDH ha señalado, el primer paso para evaluar si la afectación al derecho a la privacidad es permitida a la luz de la CADH consiste en examinar si la medida cuestionada cumple con el requisito de legalidad. Ello significa que las condiciones y circunstancias generales conforme a las cuales se autoriza una restricción al ejercicio de un derecho humano determinado deben estar claramente establecidas por ley[20]. La norma que establece la restricción debe ser una ley en el sentido formal y material[21] .

En consonancia con lo anterior, la Segunda Sala de la SCJN ha reconocido, al resolver por unanimidad el ***Amparo en Revisión 888/2017***[22] 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.

Asimismo, el Relator Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de expresión y la Relatora Especial para la Libertad de Expresión de la

---

[18] Artículos 6 de la LFPDPPP y 16 de la LGPDPPSO.
[19] Artículos 3, fracción XVI, 74, 75, 76, 77, 78 y 79 de la LGPDPPSO.
[20]Corte IDH. “Caso Escher y otros vs Brasil”. Sentencia de 6 de julio de 2009, párr. 130.
[21] La Expresión "Leyes" en el Artículo 30 de la Convención Americana sobre Derechos Humanos. Opinión Consultiva OC-6/86 de 9 de mayo de 1986. Serie A. No. 6, párrs. 27 y 32; Corte IDH “Caso Tristán Donoso vs Panamá” Sentencia del 27 de enero de 2009. par. 55; Corte IDH “Caso Escher y otros vs Brasil” Sentencia de 6 de julio de 2009, párr. 130.
[22]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

Comisión Interamericana de Derechos Humanos (en adelante "CIDH") en la Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión, ha resaltado que:

> *"Los Estados deben garantizar que la intervención, recolección y uso de información personal (...)* ***estén claramente autorizadas por la ley*** *a fin de proteger a la persona contra* ***interferencias arbitrarias o abusivas en sus intereses privados****. La ley deberá establecer límites respecto a la* ***naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación.****"*

La misma relatoría ha establecido que en el contexto de intromisiones estatales en la privacidad, la ley debe ser lo suficientemente clara en sus términos para otorgar a los ciudadanos una indicación adecuada respecto de las condiciones y circunstancias en que las autoridades están facultadas para recurrir a dichas medidas.[23]

De igual manera, el TEDH ha señalado que la ley debe ser lo suficientemente clara en sus términos para otorgar a los ciudadanos una indicación adecuada respecto de las condiciones y circunstancias en que las autoridades están facultadas para recurrir a dichas medidas.[24] Además, ha señalado que en vista del riesgo de abuso que cualquier intromisión encubierta implica, las medidas deben basarse en una ley que sea particularmente precisa, en vista de que la tecnología disponible para realizar esas actividades continuamente se vuelve más sofisticada[25].

En igual sentido, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos señaló recientemente que:

> *"Las normas legales vagas o ambiguas que otorgan facultades discrecionales muy amplias son incompatibles con la Convención Americana, porque pueden sustentar potenciales actos de arbitrariedad que se traduzcan en la violación del derecho a la privacidad o del derecho a la libertad de pensamiento y expresión garantizados por la Convención."* [26]

Con posterioridad al análisis de legalidad, tanto la SCJN como órganos internacionales de protección de derechos humanos como la Corte IDH y el TEDH coinciden en las interferencias con el derecho a la privacidad y protección de datos personales deben satisfacer los requisitos del ***test de proporcionalidad***, por virtud del cual debe corroborarse, según ha señalado la Primera Sala al resolver el **Amparo en Revisión 237/2014**, lo siguiente: "(i) que la intervención legislativa persiga un fin constitucionalmente válido; (ii) que la medida resulte idónea para satisfacer en alguna medida su propósito

---

[23] Corte IDH. *Caso Escher y otros vs. Brasil*. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C No. 200.
[24] TEDH. *Caso de Uzun vs. Alemania*. Aplicación No. 35623/05. Sentencia de 2 de Septiembre de 2010, párr. 61; Caso de *Valenzuela Contreras vs. España*. Aplicación No. 58/1997/842/1048. Sentencia de 30 de Julio de 1998, párr. 46.
[25] TEDH. *Caso de Uzun vs. Alemania*. Aplicación No. 35623/05. Sentencia de 2 de Septiembre de 2010, párr. 61; *Weber y Sarabia vs. Alemania.* Aplicación No. 54934/00. Decisión de 29 de Junio de 2006. párr. 93.
[26] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II.

constitucional; (iii) que no existan medidas alternativas igualmente idóneas para lograr dicho fin, pero menos lesivas para el derecho fundamental; y, (iv) que el grado de realización del fin perseguido sea mayor al grado de afectación provocado al derecho fundamental por la medida impugnada"[27].

En particular, respecto de interferencias en el derecho a la privacidad y a la protección de datos personales con fines relacionados a tareas de seguridad y justicia, la LGPDPSO limita de manera reforzada la obtención y tratamiento de datos personales para estos fines al señalar en su artículo 80 que dicha obtención y tratamiento "está limitada a aquellos supuestos y categorías de datos que resulten **necesarios y proporcionales** para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos".

Igualmente, resulta pertinente destacar que tribunales y organismos internacionales de protección de derechos humanos han destacado que la existencia de salvaguardas adecuadas y efectivas resulta determinante para el análisis respecto de la necesidad y proporcionalidad de legislaciones que facultan invasiones a la privacidad de manera encubierta por parte del Estado.[28] La relevancia de garantías efectivas en contra del abuso de medidas invasivas en la privacidad ha sido destacada por la Asamblea General de la Organización de las Naciones Unidas[29], el Relator Especial de la ONU para el Derecho a la Libertad de Expresión y Opinión[30], la Alta Comisionada para los Derechos Humanos de la ONU[31], la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana sobre Derechos Humanos[32], así como por organizaciones de la sociedad civil y expertos que han recogido las mejores prácticas derivadas de la jurisprudencia y doctrina comparada

---

[27] Amparo en revisión 237/2014. Aprobado por la Primera Sala con mayoría de votos en sesión del día 4 de noviembre de 2015. De esta ejecutoria derivó la Tesis 1a. CCLXIII/201 (10a) con rubro "TEST DE PROPORCIONALIDAD. METODOLOGÍA PARA ANALIZAR MEDIDAS LEGISLATIVAS QUE INTERVENGAN CON UN DERECHO FUNDAMENTAL" Rubro: 2013156

[28] TEDH. *Caso de la Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev vs. Bulgaria*. Aplicación No. 62540/00. Sentencia de 28 de Junio de 2007; *Caso Weber y Sarabia vs. Alemania*. Aplicación No. 54934/00. Decisión de 29 de Junio de 2006.

[29] Asamblea General de la Organización de las Naciones Unidas. Resolución A/RES/68/167 sobre el derecho a la privacidad en la era digital. 18 de Diciembre de 2013.

[30] ONU. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión* Frank La Rue. 17 de abril de 2013. A/HRC/23/40, párr. 81: "*La legislación debe estipular que la vigilancia estatal de las comunicaciones debe ocurrir únicamente bajo las circunstancias más excepcionales y exclusivamente bajo la supervisión de una autoridad judicial independiente. Salvaguardas deben ser articuladas en la ley en relación a la naturaleza, alcance y duración de las posibles medidas, los motivos necesarios para ordenarlas, las autoridades competentes para autorizar, llevar a cabo y supervisarlas, y el tipo de recursos previstos en la ley para obtener una reparación*".

[31] OACNUDH. *El derecho a la privacidad en la era digital*. 30 de Junio de 2014. A/HRC/27/37, párr. 37: "*El artículo 17, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos establece que toda persona tiene derecho a la protección de la ley en contra de interferencias o ataques ilegales o arbitrarios. La "protección de la ley" debe ser otorgada a través de salvaguardas procesales efectivas, incluyendo arreglos institucionales efectivos y financiados adecuadamente. Es claro, sin embargo, que la falta de supervisión efectiva ha contribuido a una falta de rendición de cuentas por intrusiones arbitrarias o ilegales en el derecho a la privacidad en el entorno digital. Salvaguardas internas, sin monitoreo independiente externo, han demostrado ser particularmente inefectivas contra métodos de vigilancia ilegales o arbitrarios. Mientras estas salvaguardas pueden tomar una variedad de formas, el involucramiento de todos los niveles de gobierno en la supervisión de programas de vigilancia, al mismo tiempo que una supervisión por parte de una agencia civil independiente, es esencial para asegurar una efectiva protección de la ley"*.

[32] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II.

y han elaborado los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*[33].

Una de las salvaguardas fundamentales para inhibir los riesgos de abuso de invasiones encubiertas en la privacidad es el control judicial. La relevancia fundamental del control judicial previo o inmediato de medidas que invaden la privacidad de las personas ha sido resaltada recientemente por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, la cual ha señalado que:

> *"Las decisiones de realizar tareas de vigilancia que invadan la privacidad de las personas deben ser autorizadas por autoridades judiciales independientes, que deben dar cuenta de las razones por las cuales la medida es idónea para alcanzar los fines que persigue en el caso concreto; de si es lo suficientemente restringida para no afectar el derecho involucrado más de lo necesario; y de si resulta proporcional respecto del interés que se quiere promover"*[34].

Igualmente, se han reconocido otras salvaguardas indispensables para inhibir los riesgos inherentes de abuso de las medidas de vigilancia encubierta, como lo son la supervisión independiente, las medidas de transparencia o el derecho de notificación al afectado.

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana ha señalado que "los Estados deben establecer mecanismos de supervisión independientes sobre las autoridades encargadas de realizar las tareas de vigilancia"[35]. En igual sentido, en la resolución "*El derecho a la privacidad en la era digital*", adoptada por consenso por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013, se recomienda a los Estados establecer o mantener "mecanismos nacionales de supervisión independiente y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado"[36] Por su parte, el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas ha expresado que:

> *"Los Estados deben ser completamente transparentes respecto del uso y alcance de los poderes y técnicas de vigilancia de las comunicaciones. Deben publicar, como mínimo, información agregada sobre el número de solicitudes aprobadas y rechazadas, una desagregación de las solicitudes por proveedor de servicios y por investigación y propósito.*
>
> *Los Estados deben otorgar a los individuos suficiente información para permitirles comprender totalmente el alcance, naturaleza y aplicación de leyes que permiten la vigilancia de comunicaciones. Los Estados deben permitir a los proveedores de*

[33] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. 10 de mayo de 2014. Disponible en: https://necessaryandproportionate.org/es/principios/
[34] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 165.
[35] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II, párr. 170
[36] ONU. Asamblea General. Resolución aprobada por la Asamblea General el 18 de diciembre de 2013. 68/167. El derecho a la privacidad en la era digital. A/RES/68/167. 21 de enero de 2014.

servicios la publicación de los procedimientos que aplican para manejar la vigilancia de comunicaciones estatal, adherirse a esos procedimientos, y publicar registros sobre la vigilancia de comunicaciones estatal. (...)"[37].

Otra de las salvaguardas fundamentales para proteger el derecho a la vida privada, garantizar el debido proceso y el acceso a un recurso efectivo es el derecho de notificación a la persona afectada. Es decir, la obligación de parte de la autoridad de notificar a una persona que su privacidad o datos personales fueron interferidos mediante una medida de vigilancia encubierta. Si bien, dicha notificación, puede no poder llevarse a cabo de manera previa o inmediata, en tanto se podría frustrar el éxito de una investigación, dicha notificación debe llevarse a cabo cuando no esté en riesgo una investigación, no exista riesgo de fuga, de destrucción de evidencia o el conocimiento pueda generar un riesgo inminente de peligro a la vida o integridad personal de alguna persona.

Este derecho de notificación a las personas afectadas por medidas de vigilancia ha sido reconocido, por ejemplo, por el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas:

> *"**Los individuos deben contar con el derecho a ser notificados que han sido sujetos de medidas de vigilancia** de sus comunicaciones o que sus comunicaciones han sido accesadas por el Estado. Reconociendo que la notificación previa o concurrente puede poner en riesgo la efectividad de la vigilancia, los individuos deben ser notificados, en cualquier caso, una vez que la vigilancia ha sido completada y se cuenta con la posibilidad de buscar la reparación que proceda respecto del uso de medidas de vigilancia de las comunicaciones"*[38]

Este derecho de notificación ha sido reconocido, además, por el TEDH, el cual determinó en el ***Caso Ekimdziev vs. Bulgaria*** que una vez que la vigilancia ha cesado y ha transcurrido el tiempo estrictamente necesario para que el propósito legítimo de la vigilancia no sea puesto en riesgo, la notificación al afectado debe llevarse a cabo sin dilación[39].

De manera particularmente relevante para el presente caso, resulta pertinente destacar la sentencia del TEDH en el caso ***S. y Marper vs. Reino Unido***[40], en donde consideró que la recolección y conservación masiva e indiscriminada de datos biométricos, como huellas digitales y datos genéticos, como muestras de ADN, constituye una interferencia desproporcionada e innecesaria del derecho a la privacidad y la protección de datos personales.

En el mencionado precedente, el TEDH resalta la importancia de la protección de los datos personales para el disfrute del derecho del respeto a la vida privada y familiar de una persona, por lo cual "**[l]a legislación nacional debe ofrecer las salvaguardias adecuadas**

---

[37] Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. 17 de Abril de 2013. A/HRC/23/40
[38] Ídem.
[39] TEDH. *Caso de la Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev vs. Bulgaria.* Aplicación No. 62540/00. Sentencia de 28 de Junio de 2007.
[40] TEDH. Caso *"S. and Marper vs. United Kingdom"* Aplicación No. 30562/04. Sentencia del 04 de diciembre de 2008. Párr. 67

para evitar cualquier uso de los datos personales que pueda ser incompatible con las garantías de este artículo 8 de la Convención*"*[41]*.*

Así, el TEDH reconoce que dichas salvaguardas son más necesarias **"en lo que respecta a la protección de los datos personales sometidos a tratamiento automático, sobre todo cuando dichos datos se utilizan con fines policiales"***[42]*.*

Por lo cual, el TEDH señala que: "**[l]a legislación nacional debería garantizar, en particular, que dichos datos sean pertinentes y no excesivos en relación con los fines para los que se almacenan; y conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para el fin para el que se almacenan esos datos"**[43]**.** Asimismo, recalca que dentro de las garantías reconocidas por la legislación nacional deben de incluirse que **"los datos personales conservados estén protegidos eficazmente contra el uso indebido y el abuso** (...). **Las consideraciones anteriores son especialmente válidas en lo que respecta a la protección de categorías especiales de datos más sensibles**"[44].

Igualmente, deben destacarse también el criterio del Tribunal de Justicia de la Unión Europea (en adelante "TJUE") en el ***Caso "Digital Rights Ireland***" donde consideró que las medidas que obligan a la recolección y conservación masiva e indiscriminada de datos personales son incompatibles con el derecho a la privacidad y a la protección de datos. Por ejemplo, en el citado caso, el TJUE, señaló que la legislación que ordenaba medidas de recolección y almacenamiento masiva e indiscriminada de datos conservados de telefonía celular con el fin de prevenir e investigar la delincuencia: "**afecta con carácter global a todas las personas que utilizan servicios de comunicaciones electrónicas, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales**. Por lo tanto, **se aplica incluso a personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con delitos graves**. Además, **no establece ninguna excepción, por lo que se aplica también a personas cuyas comunicaciones están sujetas al secreto profesional con arreglo a las normas de la legislación nacional"**[45].

Respecto a la finalidad que perseguía esta legislación consistente en combatir la lucha contra la delincuencia, el TJUE argumenta que:

I. ***"No exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública*** *y, en particular, l****a conservación no se limita a datos referentes a un período temporal o zona geográfica determinados o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la***

[41] Ibídem. Traducción propia. Párr. 103
[42] Idem.
[43] Idem.
[44] Ibídem, párr. 103 Traducción propia.
[45] 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. Par. 58 Consulta: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN

conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos graves". [46]

II. [Aludiendo a la falta de límites de la legislación]: "***no fija ningún criterio objetivo que permita delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que, debido a la magnitud y la gravedad de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, puedan considerarse suficientemente graves para justificar tal injerencia***".[47]

El TJUE concluye que dicha legislación no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales los derechos fundamentales de los ciudadanos al respeto de la vida privada y de las comunicaciones y a la protección de los datos de carácter personal reconocidos en la Carta de Derechos Fundamentales de la Unión Europea. Por lo cual, el Tribunal resolvió que dicha legislación constituye "**una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión**, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario."[48]

Posteriormente, tras resolver el ***caso de Digital Rights Ireland***, el tribunal resolvió los casos conjuntos en el ***caso Watson y otros***[49] donde también se combatían normas nacionales donde se preveía la retención de datos conservados de telefonía de manera masiva e indiscriminada como una medida contra la delincuencia.

Sobre estos casos, el TJUE, resolvió que: si bien es cierto que la eficacia de **la lucha contra la delincuencia grave**, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, **no puede por sí solo justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada** de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha[50]".

Así, el Tribunal reitera que una normativa nacional que cubra "**de manera generalizada a todos los abonados y usuarios registrados** y que tiene por objeto todos los medios de comunicación electrónica así como todos los datos de tráfico, **no establece ninguna diferenciación, limitación o excepción en función del objetivo que se pretende lograr**".[51]

En ese sentido, el TJUE sostuvo que una norma que obligue el almacenamiento de datos conservados de manera masiva "**afecta globalmente a todas las personas que hacen**

---

[46] Ibídem, párr. 59.
[47] Ibídem, párr. 60.
[48] Ibídem, párr 66.
[49] TJUE. *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson*. Casos Conjuntos, C-203/15 y C-698/15, 21 de diciembre de 2016. Consulta en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1088733
[50] Ibídem, párr. 103.
[51] Ibídem, párr. 105

uso de servicios de comunicaciones electrónicas, aunque no se encuentren, ni siquiera indirectamente, en una situación que justifique una acción penal. Por tanto, esa normativa **se aplica incluso a las personas de las que no existe ningún indicio para pensar que su comportamiento pueda tener una relación, incluso indirecta o remota, con la comisión de delitos graves**".[52]

Igual que el caso predecesor, el TJUE señala la falta de salvaguardas en este tipo de normativas ya que: **"no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública**. En particular, **no está limitada a una conservación de datos referentes a un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia.[53]"**

En conclusión, El TJUE resuelve que este tipo de legislación "**excede, por tanto, de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática"** [54].

B. Aplicación del parámetro de regularidad constitucional

En atención al marco jurídico de protección del derecho a la privacidad y de protección de datos personales que ha sido desarrollado, es claro que las normas combatidas, al disponer la recolección y conservación masiva y obligatoria de datos personales, incluyendo datos personales sensibles como lo son los datos biométricos, así como disponer que autoridades puedan tener acceso a los mismos, constituyen de manera innegable interferencias en el derecho a la privacidad y a la protección de datos personales.

En este sentido, a continuación se exponen los argumentos con los que se demuestra que las normas combatidas incumplen con los requisitos que el parámetro de regularidad constitucional exige.

1. <u>Incumplimiento del requisito de legalidad</u>

Como fue desarrollado anteriormente, para que una interferencia en el derecho a la privacidad y la protección de datos personales pueda ser considerada compatible con el marco constitucional, resulta indispensable que dicha interferencia cumpla el requisito de legalidad, lo cual implica analizar si la interferencia se encuentra autorizada por una ley, en el sentido formal y material, creada en cumplimiento del marco jurídico y estableciendo con claridad suficiente la sustancia, contenido y alcance del derecho a la privacidad y a la protección de datos personales.

En este sentido, las normas combatidas incumplen con el requisito de legalidad, al menos, en dos sentidos. Primero, al crear el PANAUT sin realizar una Evaluación de Impacto en la

[52] Ídem.
[53] Ibídem, párr. 106.
[54] Ibídem, párr 107.

Privacidad (EIP) como lo exige la LGPDPSO y en segundo lugar, al 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, como lo es la definición específica de los datos biométricos que obligatoriamente serán recabados como requisito para ejercer el derecho de acceso a las tecnologías de la información y la comunicación.

a) Omisión de realizar una Evaluación de Impacto en la Privacidad (EIP)

La LGPDPSO establece en su artículo 74 la obligación de realizar una Evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante "INAI") cuando se pretendan modificar políticas públicas que impliquen un "tratamiento intensivo o relevante de datos personales". El artículo 75 de la LGPDPSO, por su parte establece que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando "existan riesgos inherentes a los datos personales a tratar", "se traten datos personales sensibles", y "se efectúen o pretendan efectuar transferencias de datos personales".

En este sentido, el artículo 76 de la LGPDPSO y los artículos 8 y 9 de las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, emitidas por el INAI, establecen diversos criterios y ejemplos de tratamientos intensivos y relevantes de datos personales, entre los que se encuentran, por ejemplo "crear bases de datos concernientes a un número elevado de titulares (...) de tal manera que se produzca la acumulación no intencional de una gran cantidad de datos personales respecto de los mismos"[55], tratar datos biométricos[56] o "tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos".

La creación del PANAUT a través de la reforma y adición de diversas disposiciones a la LFTR (las normas combatidas) innegablemente constituye una modificación de políticas que implica tratamientos intensivos y relevantes, por lo que antes de la modificación de las normas debió de haberse cumplido con la obligación de realizar una EIP en los términos exigidos en la LGPDPSO. Esto es así pues el Poder Legislativo, quien figura como sujeto obligado según el artículo 1 de la LGPDPSO y que es responsable de la modificación

---

[55] Art. 9. Considerando lo dispuesto en el artículo 76 de la Ley General, se entenderá, de manera enunciativa mas no limitativa, que el responsable está en presencia de un tratamiento intensivo o relevante de datos personales, de manera particular, cuando pretenda: (...)
IV. Crear bases de datos concernientes a un número elevado de titulares, aun cuando dichas bases no estén sujetas a criterios determinados en cuanto a su creación o estructura, de tal manera que se produzca la acumulación no intencional de una gran cantidad de datos personales respecto de los mismos.; ACUERDO mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales. Publicado en el Diario Oficial de la Federación el 23 de enero de 2018.

[56] Art. 9 VIII. Permitir el acceso de terceros a una gran cantidad de datos personales que anteriormente no tenían acceso, ya sea, entregándolos, recibiendolos y/o poniéndolos a su disposición en cualquier forma;CUERDO mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales. Publicado en el Diario Oficial de la Federación el 23 de enero de 2018.

normativa, dispuso la creación del PANAUT, el cual implica el tratamiento masivo de datos personales sensibles, como lo son los datos biométricos, y la creación de la base de datos más grande de la historia del país.

No obstante lo anterior, del proceso legislativo no se desprende que antes de la emisión de las normas combatidas el Congreso de la Unión haya presentado ante el INAI la EIP, de manera que las autoridades responsables pudieran tomar en cuenta las recomendaciones del INAI antes de decidir crear el PANAUT o establecer diversas características de su diseño que ponen en mayor riesgo los derechos de todas las personas usuarias de telefonía móvil.

Por virtud de lo anterior, **las normas combatidas resultan inconstitucionales al actualizarse una primera violación al principio de legalidad derivada del incumplimiento de la obligación de presentar la EIP con anterioridad a la modificación de las normas que crean el PANAUT**.

b) Violación al principio de reserva de Ley al delegar a una autoridad administrativa la definición de aspectos sustantivos como la definición de los datos biométricos que serán recolectados y almacenados de manera obligatoria.

Las normas combatidas, 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 Instituto Federal de Telecomunicaciones (en adelante “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 normas combatidas vulneran los principios de legalidad, reserva de ley y el derecho de las quejosas de seguridad jurídica ya que las interferencias e intromisiones en la vida privada y en la protección de datos personales que las normas combatidas provocan, se pretende que sean 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.

Al respecto es pertinente hacer referencia a la Jurisprudencia P./J. 30/2007 **FACULTAD REGLAMENTARIA. SUS LÍMITES**[57] 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 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”.

[57] 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.

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 constitucional[58] 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".

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***[59], 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."

---

[58] 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

[59] 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 -

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***[60] 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 l**as normas combatidas, 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, contenido y alcance del derecho a la protección de datos personales, lo cual incumple el parámetro de regularidad constitucional, actualizándose así una segunda violación al principio de legalidad y al principio de reserva de ley que deriva en la inconstitucionalidad de las normas combatidas**.

2. Finalidad constitucionalmente válida

Con independencia de las violaciones constitucionales demostradas derivadas del incumplimiento del requisito de legalidad, a continuación se procede a la aplicación del ***test de proporcionalidad*** que, como ha sido mencionado anteriormente, es requerido por la Constitución y las normas de derechos humanos de fuente internacional para evaluar la compatibilidad de interferencias en el derecho a la privacidad y protección de datos personales con el parámetro de regularidad constitucional.

En primer lugar, deben identificarse los fines que se persiguen con la medida combatida para después poder determinar si son constitucionalmente válidos[61]. En el caso concreto se acepta que las normas combatidas persiguen una finalidad constitucionalmente válida, como lo es la seguridad pública. No obstante lo anterior, se reitera que la intencionalidad del legislador no justifica en sí misma la medida, sobre todo cuando la misma no cumple con el resto de las etapas del *test de proporcionalidad*, como a continuación se demuestra.

3. Incumplimiento del requisito de idoneidad

La segunda etapa del *test* de proporcionalidad exige examinar la idoneidad de las interferencias en el derecho a la privacidad y a la protección de datos personales para alcanzar el fin perseguido. La Primera Sala de la SCJN ha explicado que “en esta etapa del escrutinio debe analizarse si la medida impugnada tiende a alcanzar en algún grado los

[60] 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

[61] SCJN. Amparo en revisión 237/ 2014. Ponente: Arturo Zaldívar Lelo de Larrea. Aprobado por mayoría de votos. De este precedente surge la Tesis Aislada 1a. CCLXV/2016 (10a.) PRIMERA ETAPA DEL TEST DE PROPORCIONALIDAD. IDENTIFICACIÓN DE UNA FINALIDAD CONSTITUCIONALMENTE VÁLIDA. Registro 2013143

fines perseguidos por el legislador. En este sentido, el examen de idoneidad presupone la existencia de una relación entre la intervención al derecho y el fin que persigue dicha afectación, siendo suficiente que la medida contribuya en algún modo y en algún grado a lograr el propósito que busca el legislador"[62].

En este sentido, las autoridades responsables pretenden justificar la creación del PANAUT aludiendo a la supuesta utilidad que el mismo podría tener para la prevención e investigación de hechos delictivos, en tanto se argumenta que el PANAUT permitiría identificar a las personas que utilizan la telefonía móvil como instrumento de delito.

Contrario a lo señalado por las responsables, no existe evidencia alguna que permita suponer que la creación del PANAUT contribuya de forma alguna a la prevención e investigación de delitos, como lo señala un estudio de la asociación GSMA, que agrupa a más de 800 operadores de telefonía móvil en el mundo[63].

Además de resultar inverosímil y carente de toda lógica la suposición de que, por ejemplo, integrantes de grupos de la delincuencia organizada van a llevar a cabo hechos delictivos utilizando teléfonos móviles asociados a su identidad y datos biométricos, la suposición de que la persona registrada en el PANAUT es la persona responsable de una comunicación que aparente originarse desde el número asignado a dicha persona carece de evidencia.

Por el contrario, según datos de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) elaborada por el Instituto Nacional de Estadística y Geografía (INEGI), al menos un 12% de personas usuarias de telefonía móvil comparten un teléfono celular con otras personas[64].

Igualmente, las líneas de telefonía móvil registradas por personas morales únicamente permiten identificar a la persona representante legal de dicha persona moral sin que de lo anterior pueda desprenderse la identidad de la persona responsable de una comunicación que sea instrumento de un delito. En este sentido, se afirma que no puede construirse un nexo causal inequívoco entre el PANAUT y la identificación de las personas que utilizan la telefonía móvil.

Adicionalmente, es notorio que la delincuencia cuenta con múltiples maneras de eludir el registro en el PANAUT. Por ejemplo, resulta posible utilizar tarjetas SIM de otros países en los que no existe obligación alguna de registro, como Estados Unidos, Canadá, Reino Unido, Nueva Zelanda, Suecia, Finlandia, entre otros. En particular, dada la cercanía, longitud de la frontera compartida, los lazos sociales intensos y las múltiples ofertas de servicios de telefonía móvil sin cobro por *roaming* internacional, la adquisición y uso de

---

[62] SCJN. Amparo en revisión 237/ 2014. Ponente: Arturo Zaldívar Lelo de Larrea. Aprobado por mayoría de votos. De este precedente surge la Tesis Aislada 1a. CCLXVIII/2016 (10a.) "SEGUNDA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA IDONEIDAD DE LA MEDIDA LEGISLATIVA". Registro: 2013152

[63] GSMA. "Mandatory registration of prepaid SIM cards: addressing challenges through best practice" Abril, 2016. p. 2 y 17 Consulta en: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

[64] INEGI. "Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2019". 2019. Consulta en: https://www.inegi.org.mx/programas/dutih/2019/#Tabulados

tarjetas SIM provenientes de los Estados Unidos resulta sumamente accesible, por lo que resulta sencillo realizar comunicaciones respecto de las cuales el PANAUT no ofrece información alguna que permita la identificación del origen de la comunicación.

Igualmente, existe amplia evidencia de la factibilidad de ataques que permiten suplantar (*swapping)*, duplicar o clonar una tarjeta SIM. Incluso, autoridades reguladoras de las comunicaciones como la *Federal Communications Commission* (FCC)[65] de los Estados Unidos han advertido sobre los riesgos de estos ataques, los cuales permiten a una persona realizar y recibir comunicaciones suplantando una tarjeta SIM adquirida y utilizada legalmente por otra persona. De esta manera, es previsible que tras la conformación del PANAUT, la delincuencia recurra al robo, clonación, duplicación o *swapping* de tarjetas SIM para realizar comunicaciones que aparenten haber sido realizadas por personas distintas registradas en el PANAUT.

Asimismo, existen múltiples servicios de Voz sobre el Protocolo de Internet (VOIP)[66] que permiten la realización de llamadas y el envío de mensajes SMS a través de Internet sin necesidad de una tarjeta SIM ni de registro en el PANAUT. Inclusive, los servicios VOIP permiten a una persona usuaria elegir el número que aparecerá en el identificador de llamadas del destinatario de la comunicación, lo cual podría, de manera similar a otras técnicas de suplantación mencionadas anteriormente, permitir a la delincuencia realizar llamadas que aparenten haber sido realizadas por personas distintas registradas en el PANAUT.

De esta manera, frente a la ausencia de evidencia de que requisitos de identidad para la adquisición y uso de tarjetas SIM contribuyan a la reducción de índices delictivos; frente a la imposibilidad de presumir que la persona registrada en el PANAUT es la responsable de la comunicación; y dado que existen múltiples maneras en las que puede eludirse el PANAUT, es evidente que **las normas combatidas incumplen el requisito de idoneidad al no contribuir de manera alguna a la seguridad pública, por lo que se actualiza de nuevo la inconstitucionalidad de las mismas.**

No obstante lo anterior, aún en el caso de que se considere que las normas combatidas contribuyen ínfimamente a la consecución de la finalidad perseguida, resulta pertinente analizar las siguientes etapas del *test* de proporcionalidad a manera de comprobar que las invasiones a la privacidad y a la protección de datos personales provocadas por las normas combatidas son innecesarias y desproporcionadas.

4. Incumplimiento del requisito de necesidad

En la tercera etapa del *test* de proporcionalidad corresponde analizar si la interferencia en el derecho a la privacidad y protección de datos personales es necesaria o si, por el contrario,

---

[65] FCC. “Fraude con Teléfonos Celulares”. 23 de abril de 2020. Consulta en: https://www.fcc.gov/consumers/guides/fraude-con-telefonos-celulares

[66] Ver: “Yúbal Fernández. “VOIP: ¿Qué es y cómo funciona? “ Xataka. 12 de octubre de 2019. Consulta en: https://www.xataka.com/basics/voip-que-como-funciona

existen medidas alternativas que sean idóneas pero que afecten en menor grado el derecho fundamental.

De esta manera, según la Primera Sala de la SCJN “el examen de necesidad implica corroborar, en primer lugar, si existen otros medios igualmente idóneos para lograr los fines que se persiguen y, en segundo lugar, determinar si estas alternativas intervienen con menor intensidad el derecho fundamental afectado. Lo anterior supone hacer un catálogo de medidas alternativas y determinar el grado de idoneidad de éstas, es decir, evaluar su nivel de eficacia, rapidez, probabilidad o afectación material de su objeto”[67].

Del proceso legislativo se desprende que para las comisiones dictaminadoras de la Cámara de Diputados y de la Cámara de Senadores, “*la función principal de la elaboración del [PANAUT] tiene como objetivo la identificación plena y certera de los titulares de las líneas de comunicación; con la creación de esta figura, las autoridades competentes tendrán más elementos normativos para identificar la comisión de un delito a través de equipos móviles*”[68]
.
A pesar de que como fue demostrado en la etapa de idoneidad, el PANAUT no es idóneo para identificar a las personas remitentes de una comunicación, ni ofrece a las autoridades competentes ningún elemento para “identificar la comisión de un delito”, para efectos del análisis de necesidad resulta pertinente identificar alternativas idóneas para conseguir los fines perseguidos.

En este sentido, debe señalarse que las autoridades de seguridad y procuración de justicia competentes, ya cuentan con un amplio catálogo de técnicas de investigación que les permiten obtener elementos considerablemente más útiles para identificar a las personas responsables de comunicaciones vía telefonía móvil involucradas en un hecho delictivo:

- Geolocalización en tiempo real de equipos de comunicación móvil: El artículo 303 del Código Nacional de Procedimientos Penales (en adelante “CNPP”) y el artículo 9, fracción XXVI de la Ley de la Guardia Nacional (en adelante “LGN”) establecen la posibilidad de obtener, con control judicial, la localización geográfica en tiempo real de un equipo de comunicación móvil, la cual aporta elementos objetivos para la identificación de la persona que realiza las comunicaciones a través de dicho equipo.

- Acceso a datos conservados: El CNPP y la LGN permiten a las autoridades competentes acceder, con control judicial, al registro de comunicaciones establecido en el artículo 190, fracción II, el cual incluye datos como los números de origen y destino, fecha, hora y duración de cada comunicación, la ubicación digital del posicionamiento geográfico de las líneas telefónicas, los números IMEI e IMSI que identifican al teléfono móvil y a la tarjeta SIM respectivamente, entre otros datos que significativamente aportan mayores elementos para la investigación de hechos

[67] Primera Sala de la Suprema Corte de Justicia de la Nación. Amparo en revisión 237/ 2014. Ponente: Arturo Zaldívar Lelo de Larrea. Aprobado por mayoría de votos. De esta sentencia se emitió la Tesis Aislada CCLXX/2016 (10a.) “TERCERA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA NECESIDAD DE LA MEDIDA LEGISLATIVA.” Registro: 2013154

[68] Dictamen Diputados Ciudad de México, jueves 10 de diciembre de 2020. Gaceta No. 5670-IV pág. 115. Dictamen Senado Ciudad de México., a jueves 8 de abril de 2021. Gaceta No. LXIV/3SPO-126/116718 pág. 3.

delictivos y para la identificación de las personas que realmente realizan una comunicación a través de la telefonía móvil.

- Intervención de comunicaciones privadas: El CNPP y la LGN también permiten a las autoridades competentes obtener la autorización judicial federal para llevar a cabo la intervención de comunicaciones privadas, la cual puede aportar mayores elementos para la identificación de los comunicantes, así como respecto de los hechos delictivos realizados a través de la telefonía móvil.

- Bloqueo de señales de telefonía móvil en centros penitenciarios: El artículo 190 fracción VIII de la LFTR reconoce la posibilidad de anular de manera permanente las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen dentro del perímetro de centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores, federales o de las entidades federativas. Lo anterior resulta una medida considerablemente más idónea para prevenir la comisión de delitos a través de la telefonía móvil que el PANAUT, en tanto la aplicación de esta medida evitaría la comisión de un gran número de delitos que se encuentra documentado[69] ocurren desde centros penitenciarios.

- Otras alternativas de registro: *Ad cautelam*, se advierte que incluso si se considerara que obligaciones de registro masivas e indiscriminadas de la totalidad de las personas usuarias de telefonía móvil como el PANAUT fueran idóneas, necesarias y proporcionales frente a derechos como la privacidad, protección de datos personales, acceso a las TIC o libertad de expresión, lo cual no se considera que sea el caso, es preciso analizar alternativas que tienen un mismo nivel de idoneidad (o falta de idoneidad) pero representan considerablemente menores riesgos para el derecho a la privacidad y la protección de datos personales.

  En este sentido, debe apreciarse que el PANAUT dispone la creación de una nueva base de datos centralizada a cargo del IFT que deberá incluir, según el artículo 180 Ter de la LFTR, un amplio listado de datos personales recolectados por los concesionarios y autorizados, incluyendo el nombre, domicilio, número de identificación oficial o Clave Única de Registro de Población (CURP) y datos biométricos de la persona usuaria, los cuales pueden incluir la huella digital, el iris ocular, voz, marco facial, entre otros.

  El proceso de recolección y almacenamiento centralizado y masivo de los datos implica un riesgo alto y permanente de vulneración, el cual se agrava aún más respecto de los datos biométricos, los cuales, al referirse a características físicas y fisiológicas inmutables e inseparables a las personas, implican que en caso de la

[69] IFT. "Informe de resultados del comité especializado de estudios e investigaciones que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas para la seguridad nacional: Estudio estadístico del número de terminales móviles y de llamadas de móviles y de casetas telefónicas públicas que operan dentro de una muestra de penales en el país" . 2 de Octubre de 2018. Pág. 116 Consulta en: http://sil.gobernacion.gob.mx/Archivos/Documentos/2018/10/asun_3745953_20181004_1538661845.pdf

vulneración de esos datos, las personas podrían acarrear consecuencias graves de manera permanente e irreversible.

De esta manera, debe afirmarse que existen alternativas que permiten identificar a las personas usuarias contratantes al momento de la celebración del contrato y con posterioridad para efectos de investigación, sin la necesidad de crear una base de datos centralizada de datos biométricos de la totalidad de usuarios de telefonía móvil. Por ejemplo, puede resultar suficiente la presentación de un documento de identificación oficial aunado a la verificación de la autenticidad del documento de identidad o la verificación de que la persona que presenta el documento es la misma a aquella registrada ante el emisor de dicho documento. De esta manera no se crea una nueva base de datos biométrica, multiplicándose los riesgos de vulneración, sino que, en su caso, se aprovecha la existencia de bases de datos existentes para únicamente verificar si la persona que presenta un documento de identidad es realmente la persona registrada por el emisor del documento.

Cabe mencionar que el Instituto Nacional Electoral (INE) ya ofrece un servicio de verificación de información de la Credencial para Votar que permite validar la vigencia y coincidencia de los datos de la Credencial para Votar que presenten los ciudadanos para identificarse ante un ente público o privado[70], sin necesidad de que dichos entes recaben y conserven datos biométricos y sin que el INE transfiera dichos datos a los entes.

Una vez identificados medios igual o más idóneos que el PANAUT para la prevención e investigación de delitos cometidos a través de la telefonía móvil, corresponde analizar si dichas alternativas intervienen con menor intensidad en los derechos a la privacidad y protección de datos personales.

En este sentido, es claro que medidas como la geolocalización en tiempo real de equipos de comunicación móvil, el acceso a datos conservados y la intervención de comunicaciones privadas, al únicamente afectar de manera focalizada a un número limitado de personas respecto de las cuales existan indicios de organización o participación de hechos delictivos determinado, interfieren con menor intensidad los derechos en juego.

Además estas medidas cuentan con control judicial previo o inmediato, por lo que afectan en menor medida los derechos a la privacidad y la protección de datos personales que las normas combatidas, en las que se contempla la recolección y almacenamiento indiscriminado de datos personales, incluyendo datos personales sensibles, de la totalidad las personas usuarias de telefonía móvil.

[70] Central Electoral. “INE colabora con instituciones bancarias para prevenir el robo de identidad y fraudes a partir de la identificación de huellas dactilares”. 17 de febrero de 2019. Consulta en: https://centralelectoral.ine.mx/2019/02/17/ine-colabora-instituciones-bancarias-prevenir-robo-identidad-los-fraudes-partir-la-identificacion-huellas-dactilares/

El número total de personas usuarias de telefonía móvil según la ENDUTIH 2019, asciende a más de 86.5 millones de personas[71], permitiéndose el acceso a dicha base de datos por parte de autoridades de seguridad y procuración de justicia sin que se establezca control judicial o ninguna otra salvaguarda adecuada y sin establecer ningún tipo de límite material respecto de los hechos delictivos o las circunstancias respecto de las cuales puede accederse a PANAUT.

De igual manera, el bloqueo de señales de telefonía móvil en centros penitenciarios resulta una medida que no afecta en absoluto la privacidad y la protección de datos personales de los usuarios de telefonía móvil y por el contrario ofrece una gran eficacia para prevenir la comisión de delitos cometidos a través de la telefonía móvil, en virtud de la evidencia que existe respecto de la prevalencia de la comisión de este tipo de delitos desde los centros penitenciarios.

Finalmente, se advierte que alternativas de registro y validación de la identidad que no implican la recolección y almacenamiento de datos biométricos en una nueva base de datos centralizada, ni su acceso por parte de autoridades sin control judicial u otras salvaguardas, como se pretende con la creación del PANAUT, resultan ser menos invasivas en los derechos a la privacidad y la protección de datos personales y ofrecen la misma idoneidad, o falta de ella, para facilitar la prevención e investigación de hechos delictivos cometidos utilizando la telefonía móvil.

De esta manera, se corrobora que **la creación y operación del PANAUT no cumple con el requisito de necesidad, al existir medidas alternativas que resultan ser más idóneas para conseguir el fin perseguido y que afectan en menor medida los derechos a la privacidad y la protección de datos personales, por lo tanto se confirma la inconstitucionalidad de las normas combatidas**.

No obstante lo anterior, resulta pertinente analizar las siguiente etapa del *test* de proporcionalidad a manera de comprobar que las invasiones a la privacidad y a la protección de datos personales provocadas por las normas combatidas son desproporcionadas en cualquier caso.

5. Incumplimiento del requisito de proporcionalidad en sentido estricto

En la cuarta etapa del *test de proporcionalidad* corresponde llevar a cabo finalmente un examen de proporcionalidad en sentido estricto. La Primera Sala de la SCJN ha explicado que esta grada del test “consiste en efectuar un balance o ponderación entre dos principios que compiten en un caso concreto. Dicho análisis requiere comparar **el grado de intervención en el derecho fundamental que supone la medida legislativa examinada, frente al grado de realización del fin perseguido por ésta**. En otras palabras, en esta

[71] IFT. “En México hay 80.6 millones de usuarios de internet y 86.5 millones de usuarios de teléfonos celulares: ENDUTIH 2019. 17 de febrero”. 17 de febrero de 2020 . Consulta en: http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/en-mexico-hay-806-millones-de-usuarios-de-internet-y-865-millones-de-usuarios-de-telefonos-celulares

fase del escrutinio es preciso realizar una ponderación entre los beneficios que cabe esperar de una limitación desde la perspectiva de los fines que se persiguen, frente a los costos que necesariamente se producirán desde la perspectiva de los derechos fundamentales afectados. De este modo, **la medida impugnada sólo será constitucional si el nivel de realización del fin constitucional que persigue el legislador es mayor al nivel de intervención en el derecho fundamental.** En caso contrario, la medida será desproporcionada y, como consecuencia, inconstitucional"[72].

En este sentido, resulta procedente analizar en primer término el grado de afectación a los derechos a la privacidad y a la protección de datos personales para posteriormente ponderar dicha afectación frente al nivel de realización del fin constitucional que persiguen las normas combatidas.

Del análisis de las normas combatidas se desprenden diversas características del PANAUT que resultan fundamentales para apreciar el **alto grado de afectación que provocan**. 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 no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con la comisión de delitos. Al respecto resulta pertinente recordar los precedentes del TJUE en los casos *Digital Rights Ireland*[73] y Watson vs Reino Unido[74] 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 combatidas predeterminan el diseño centralizado de la base de datos del PANAUT, es decir, obligan al almacenamiento en una sola base 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 se agravan significativamente al incluirse a los datos biométricos como parte de la base de datos. Como ha sido mencionado, los datos biométricos se refieren a las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, que permiten o confirman la identificación

---

[72] SCJN. Primera Sala. *Amparo en Revisión 237/2014*. Aprobado por mayoría de votos en sesión del 25 de noviembre de 2016. Ponente: Arturo Zaldívar Lelo de Larrea. De esta sentencia derivó la tesis aislada 1a. CCLXXII/2016 (10a.)con rubro: "CUARTA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA PROPORCIONALIDAD DEL SENTIDO ESTRICTO DE LA MEDIDA". Registro 2013136

[73] 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.

[74] 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.

única de una persona[75]. 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 indisociablemente 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 persona[76].

Por otro lado, debe tomarse en cuenta que la característica de obligatoriedad del registro en el PANAUT, que dispone el artículo 180 Quáter de la LFTR, representa una interferencia severa en 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 que sea ejercido si se renuncia a la posibilidad de acceder a la telefonía móvil, e inclusive, se dispone en ese caso que los datos seguirán siendo almacenados por seis meses.

Igualmente las normas combatidas anulan de manera absoluta el principio de consentimiento, en tanto se condiciona el ejercicio del derecho de acceso a las TIC a aceptar el tratamiento de datos personales, lo cual no cumple con los requisitos de libertad necesarios para constituir un consentimiento real. Lo mismo sucede respecto del principio de calidad y proporcionalidad en tanto no se establecen límites temporales al tratamiento de las personas usuarias ni se minimizan los tratamientos a lo estrictamente necesario.

Por otra parte, como fue mencionado al desarrollar el marco jurídico de protección del derecho a la privacidad y la protección de datos personales, es fundamental para el análisis de proporcionalidad el analizar si existen salvaguardas adecuadas para evitar el abuso de medidas invasivas, en particular cuando el Estado las lleva a cabo de manera encubierta.

En este sentido, debe destacarse que el párrafo tercero del artículo 180 Séptimus dispone que autoridades de seguridad, procuración y administración de justicia podrán acceder a la información contenida en el PANAUT sin establecer salvaguardas adecuadas y suficientes para prevenir el abuso de este acceso. En primer lugar, las normas combatidas no

---

[75] 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.

[76] 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

establecen límite alguno respecto de los casos, circunstancias, delitos, procedimientos, categorías de datos o el volumen de acceso al que las autoridades podrán tener acceso.

Igualmente, no se establece ningún mecanismo de control judicial previo o inmediato, ninguna medida de transparencia, de supervisión independiente o de notificación a las personas afectadas por los accesos al PANAUT de parte de autoridades. De esta manera, las personas respecto de las cuales la autoridad tenga acceso a sus datos personales, incluyendo datos personales sensibles, quedan en la indefensión absoluta, pues no tendrán conocimiento de que su esfera de derechos ha sido invadida y por ende no podrán incoar los mecanismos jurídicos correspondientes para resistir injerencias arbitrarias o ilegales.

Igualmente, la ausencia de control judicial y administrativo independiente evita que un tercero pueda asegurarse de que el acceso de las autoridades a la base de datos del PANAUT se encuentra debidamente fundado y motivado, con lo cual resulta imposible detectar abusos, lo cual a su vez implica que las sanciones previstas en las normas combatidas y en otros ordenamientos jurídicos, aplicables al acceso o uso ilegal o arbitrario de los datos contenidos en el PANAUT, se convierten en meras disposiciones cosméticas sin posibilidad real de disuadir o remediar abusos.

En las normas combatidas tampoco se define si las autoridades podrán tener acceso libre y en masa a todos los datos contenidos en la base de datos o si tendrán que realizar requerimientos específicos y focalizados a determinadas líneas respecto de las cuales exista algún indicio de haber participado en la organización o comisión de hechos delictivos. Lo anterior supone el riesgo de que la base de datos pueda ser utilizada para hacer el "cruce" (*cross-matching)* con otras bases de datos, lo cual puede dar pie al monitoreo y vigilancia de la población[77].

Asimismo, 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, procuración y administración 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"[78].

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 documentado[79] y reconocido por autoridades nacionales y por órganos internacionales de derechos humanos.

---

[77] Idem.
[78] 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 pár. 498.
[79] 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

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 México[80], respecto del cual diversos organismos internacionales de derechos humanos han manifestado preocupación y han realizado recomendaciones[81] y respecto del cual el INAI determinó, al resolver el procedimiento de verificación identificado con la clave INAI.3S.07.01-007/2018[82], 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 incompetentes[83], el uso ilegal y sin cumplir con el requisito de control judicial que el artículo 16 de la Constitución y las leyes exigen[84], e incluso la adquisición y uso de tecnologías de vigilancia masiva como "las antenas falsas" de telefonía[85] y sistemas que permiten "recopilación en masa de (datos de) todos los usuarios de Internet en un país"[86].

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 desplegados 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 las normas combatidas implican una interferencia en el derecho a la privacidad y protección de datos personales que constituyen afectaciones de grave intensidad y que incluso anulan por completo el ejercicio de algunos derechos.

---

[80]R3D: 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/

[81] 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

[82] 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

[83] R3D. "*El Estado de la Vigilancia: Fuera de Control*" Noviembre 2016. Consulta en: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

[84]R3D. " *PGR adquirió equipo para geolocalizar 255 mil celulares en 2018; se usó para espiar a todos los candidatos: Reporte índigo*". 5 de Junio de 2019. Disponible: https://r3d.mx/2019/06/05/pgr-equipo-espionaje-celulares-geomatrix/

[85] 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-telefonia-para-recolectar-informacion-de-personas/

[86] 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/

Lo anterior, aunado a la ausencia absoluta o significativa de contribución al fin perseguido por las medidas contempladas en las normas combatidas, derivada de la ausencia de evidencia de que requisitos de identidad para la adquisición y uso de tarjetas SIM contribuyan a la reducción de índices delictivos, la imposibilidad de presumir que la persona registrada en el PANAUT es la responsable de una comunicación y dado que existen múltiples maneras en las que este puede eludirse, como fue desarrollado en la etapa de idoneidad, implica con claridad que los costos para los derechos a la privacidad y la protección de datos personales resultan ser contundentemente mayores que los ausentes o ínfimos beneficios para la seguridad pública que ofrecen las normas combatidas.

Por todo lo previamente establecido, es claro que **las normas combatidas constituyen interferencias que incumplen el requisito de proporcionalidad respecto de los derechos a la privacidad y la protección de datos personales y por ende resultan ser inconstitucionales**.

C. Conclusión

En conclusión del presente apartado y dadas las múltiples violaciones demostradas, se reitera para mayor claridad que las normas combatidas constituyen interferencias en el derecho a la privacidad y protección de datos personales que resultan inconstitucionales en virtud de que:

1. Incumplen el requisito de legalidad al haberse omitido la realización de una EIP.
2. Incumplen el requisito de legalidad y el principio de reserva de ley al delegarse en una autoridad administrativa la definición de aspectos sustantivos como la definición de los datos biométricos que serán recolectados y almacenados de manera obligatoria.
3. Incumplen el requisito de idoneidad al no contribuir de manera alguna a la seguridad pública dada la ausencia de evidencia de que requisitos de identidad para la adquisición y uso de tarjetas SIM contribuyan a la reducción de índices delictivos. Aunado a la imposibilidad de presumir que la persona registrada es la responsable de la comunicación; y dado que existen múltiples maneras en la delincuencia puede eludir el PANAUT.
4. Incumplen el requisito de necesidad al existir medidas alternativas que resultan ser más idóneas para conseguir el fin perseguido y que afectan en menor medida los derechos a la privacidad y la protección de datos personales.
5. Incumplen el requisito de proporcionalidad estricta en tanto constituyen interferencias severas y potencialmente irreversibles en el derecho a la privacidad y protección de datos personales que no se encuentran justificadas frente a los inexistentes o ínfimos beneficios para la realización de la finalidad perseguida.

En vista de lo anterior, debe concluirse que las normas combatidas resultan violatorias de de los artículos 6, 14 y 16 de la CPEUM, 11 de la CADH y 17 del PIDCP.

SEGUNDO. EL REGISTRO OBLIGATORIO AL PANAUT COMO CONDICIÓN PARA EJERCER EL DERECHO DE ACCESO A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN, AL NO SER UNA MEDIDA IDÓNEA, NECESARIA O PROPORCIONAL, VIOLA LOS ARTÍCULOS 1, 2, 6, 7, 14 Y 16 DE LA CPEUM, 1.1, 13 Y 24 DE LA CADH, 2, 19 Y 26 DEL PIDCP.

El Decreto que contiene las normas combatidas condiciona el acceso al servicio de telefonía móvil a la aceptación del tratamiento 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, será 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 las normas combatidas, en especial las descritas en el párrafo anterior, resultan violatorias del derecho de acceso a las TIC reconocido en el artículo 6 de la CPEUM, 13 de la CADH y 19 del PIDCP en atención a las siguientes consideraciones.

D. Contenido del Derecho de Acceso a las Tecnologías de la Información y la Comunicación

El Derecho de Acceso a las TIC se encuentra reconocido en el artículo 6o, tercer párrafo de la CPEUM al señalar que "[e]l Estado garantizará 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 otros[87]. De esta forma, al ser inseparable del ejercicio pleno de determinados derechos, la CIDH ha considerado que "el acceso a internet debe garantizarse universalmente, adoptando medidas para cerrar la brecha digital, promoviendo políticas de desarrollo de infraestructura, y protegiendo en todo

[87] 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.

momento la calidad e integridad del servicio, estableciendo prohibiciones explícitas en torno a bloqueos arbitrarios, parciales o totales y ralentizaciones"[88].

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 digitales[89].

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 discriminación[90].

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 nacional[91].

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 excluídas 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.

E. Aplicación del parámetro de regularidad constitucional

En atención al marco jurídico expuesto, a continuación se desarrollan las violaciones al parámetro de regularidad constitucional respecto del derecho de acceso a las TIC y en relación con el principio de no discriminación que se generan a partir de las normas combatidas.

---

[88] 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.
[89] *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.
[90] 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.*
[91] 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.

1. Violación al principio de legalidad y reserva de ley

El artículo 190, fracción VII de la LFTR establece como obligación de los concesionarios y autorizados "realizar la suspensión inmediata del servicio de telefonía móvil cuando así lo instruya el Instituto para efectos del Padrón Nacional de Usuarios de Telefonía Móvil o la autoridad competente para hacer cesar la comisión de delitos, de conformidad con lo establecido en las **disposiciones administrativas** y legales aplicables". De esta manera se faculta a autoridades administrativas a establecer restricciones absolutas al derecho de acceso a las TIC.

No obstante lo anterior, como fue desarrollado en el concepto de invalidez primero, los principios de legalidad y de reserva de ley exigen que las restricciones a los derechos humanos sean establecidas en una ley formal y material. De esta manera, **la reforma al artículo 190, fracción VII que añadió la frase "administrativas y" resulta ser abiertamente inconstitucional**.

2. Test de proporcionalidad

Las normas combatidas interfieren con el derecho de acceso a las TIC al condicionar el acceso a la telefonía móvil a la entrega de datos personales, incluyendo datos personales sensibles como los datos biométricos y al disponer la suspensión masiva del servicio de telefonía móvil respecto de cualquier línea que no haga entrega de los datos requeridos.

En este sentido, resulta procedente llevar a cabo la aplicación del ***test de proporcionalidad*** para determinar si dichas interferencias son compatibles con el parámetro de regularidad constitucional.

En primer lugar, debe afirmarse que las consideraciones en torno al incumplimiento de los requisitos de **idoneidad y necesidad** respecto de las interferencias en el derecho a la privacidad y protección de datos personales resultan idénticamente aplicables respecto del derecho de acceso a las TIC, por lo que **debe concluirse de igual manera la inconstitucionalidad de las normas combatidas**.

No obstante, respecto a la grada de **proporcionalidad**, debe apreciarse que las interferencias con el derecho de acceso a las TIC son de una intensidad severa.

La SCJN ha señalado que la intervención en un derecho fundamental que prohíba totalmente la realización de una conducta amparada por ese derecho será más intensa que una intervención que se concrete a prohibir o a regular en ciertas condiciones el ejercicio de ese derecho[92]. Por lo tanto, una prohibición absoluta en un derecho fundamental que prohíba totalmente la realización de una conducta amparada por ese derecho será más intensa que una intervención que se limite a establecer en ciertas condiciones el ejercicio de ese derecho.

---

[92] SCJN. Primera Sala de la Suprema Corte de Justicia de la Nación. Amparo en revisión 237/ 2014. Ponente: Arturo Zaldívar Lelo de Larrea. Aprobado por mayoría de votos. p.79.

Por lo cual, en el caso en concreto, al establecerse, en el artículo 190, fracción VII de la LFTR y el artículo transitorio cuarto, la imposibilidad de acceder al servicio de telefonía móvil o la cancelación del servicio sin derecho a reactivación se anula por completo el derecho de acceso a la telefonía móvil.

Adicionalmente resulta fundamental apreciar el efecto discriminatorio que las normas combatidas tendrán en grupos de población históricamente desaventajados. La discriminación, ya sea respecto de normas o actos, puede acontecer tanto de manera directa, como indirecta. Al respecto, la jurisprudencia de la SCJN ha establecido que la discriminación indirecta significa que las leyes, las políticas o las prácticas públicas o privadas son neutras en apariencia, pero afectan desproporcionadamente a personas o grupos en situación de desventaja histórica justo en razón de esa desventaja[93] en comparación de otros en una situación análoga[94] sin que exista para ello una justificación objetiva y razonable.[95]

La Corte Interamericana de Derechos Humanos (en adelante "Corte IDH") ha precisado que el principio de derecho imperativo de protección igualitaria y efectiva de la ley y no discriminación, determina que los Estados **"deben abstenerse de producir regulaciones discriminatorias o que tengan efectos discriminatorios en los diferentes grupos de una población al momento de ejercer sus derechos"[96]**

La SCJN también ha manifestado que es necesario introducir factores contextuales o estructurales en el análisis de la discriminación para poder establecer que una norma o política pública sí genera un efecto discriminatorio en la persona aunque aparente ser neutral. Entre estos factores se ubican las relaciones de subordinación en torno al género, la identidad sexo-genérica, la orientación sexual, la clase o la pertenencia étnica; las prácticas sociales y culturales que asignan distinto valor a ciertas actividades en tanto son realizadas por grupos históricamente desaventajados, y las condiciones socioeconómicas.[97] Estos factores condicionan que una ley o política pública finalmente provoque una diferencia de trato irrazonable, injusto o injustificable de acuerdo con la situación que ocupen las personas dentro de la estructura social.[98]

La Primera Sala de la SCJN también se ha pronunciado sobre la existencia de un mandato constitucional que "prevé la existencia de una vía de acceso diferenciado para los pueblos y comunidades indígenas a los medios de comunicación". Por lo cual, "dichos grupos deben

---

[93] SCJN. *Acción de Inconstitucionalidad 8/2014*. Aprobado por mayoría de votos. Ponente: Margarita Beatriz Luna Ramos. Encargado del engrose: Alfredo Gutiérrez Ortiz Mena. Secretaria: Karla I. Quintana Osuna. p. 89 par.71 De esta sentencia derivó la Tesis aislada P. VII/2016 (10a.) emitida por el Pleno de la SCJN de rubro: "DISCRIMINACIÓN POR OBJETO Y POR RESULTADO. SU DIFERENCIA." Registro 2012597

[94] SCJN. Segunda Sala. *Amparo Directo 9/2018*, p. 32.

[95] Tesis 1ª. XLIV/2014 (10a.), emitida por la Primera Sala de esta Suprema Corte de rubro y texto: "DERECHO HUMANO A LA IGUALDAD JURÍDICA. DIFERENCIAS ENTRE SUS MODALIDADES CONCEPTUALES

[96] Cfr. *Caso Artavia Murillo y otros ("fecundación in vitro") vs. Costa Rica*. *Fondo, Reparaciones y Costas.* Sentencia de 28 de septiembre de 2012. Página 134. Párrafos 285 y 286.

[97] SCJN. Acción de Inconstitucional 8/2014, p. 90, párr. 74.

[98] Íbidem, citando a Saba, Roberto, "Desigualdad estructural", en Roberto Gargarella y Marcelo Alegre, El derecho a la igualdad. Aportes para un constitucionalismo igualitario, Buenos Aires, Lexis Nexis, 2007 y Serrano García, Sandra et al. "Herramientas para una comprensión

considerarse beneficiarios de un derecho que les permita adquirir, operar y administrar medios de comunicación, en los términos que las leyes de la materia determinen". [99]

Asimismo, la Primera Sala de la SCJN señaló en el Amparo en Revisión 622/2015, que "los derechos lingüísticos amparan el derecho de los pueblos y personas indígenas a fundar o utilizar los medios de comunicación. Por lo cual, el ejercicio de este derecho deberá hacerse en condiciones de no discriminación, y mediante la adopción de medidas por parte del Estado que lleven a asegurar la diversidad cultural en dichos medios"[100].

En este sentido, es importante considerar que según datos del año 2015 en el país, al menos un millón de personas (1,003,702) de todas las edades no cuentan con registro de nacimiento. De éstas, 903,288 personas nacieron en territorio nacional (89.9%), 93,425 nacieron en el extranjero (9.3%), mientras que el resto no especificaron su lugar de nacimiento (0.8%).[101] En igual sentido, existe un número importante de personas que no cuentan con CURP o con una identificación oficial que desproporcionadamente pertenece a grupos desaventajados históricamente como lo son las personas en situación de pobreza, las personas que habitan en comunidades rurales y las personas indígenas.

Igualmente, resulta previsible que ante los costos derivados de la implementación de las tecnologías necesarias para la recolección de datos personales sensibles, incluyendo los datos biométricos, las concesionarias de telecomunicaciones reducirán drásticamente los puntos de venta de tarjetas SIM y los ubiquen en lugares con mayor densidad poblacional, con lo cual se afecta la accesibilidad a las tecnologías de la información y la comunicación, en particular de las personas que se ubican en poblaciones remotas.

De esta manera, es claro que la exigencia de los artículos 180 Ter y 180 Quáter de la LFTR de proporcionar una identificación oficial o CURP excluirá a personas pertenecientes a grupos de población históricamente desaventajados por su situación económica, ubicación geográfica, grupos para personas indígenas y personas migrantes del acceso a las tecnologías de la información y la comunicación.

Así, dada la ausencia absoluta o significativa de contribución al fin perseguido por las medidas contempladas en las normas combatidas, derivada de la ausencia de evidencia de que requisitos de identidad para la adquisición y uso de tarjetas SIM contribuyan a la reducción de índices delictivos, la imposibilidad de presumir que la persona registrada en el PANAUT es la responsable de una comunicación y dado que existen múltiples maneras en las que este puede eludirse, como fue desarrollado en el concepto de invalidez primero, es claro que **las restricciones absolutas al derecho de acceso a las TIC, así como el efecto discriminatorio que suponen las normas combatidas, resultan ser significativamente mayores a los ausentes o ínfimos beneficios para la seguridad**

---

[99] SCJN. Primera Sala. *Amparo en revisión 603/2019*. Aprobado por unanimidad en sesión del 13 de enero de 2021. Ponente: Alfredo Gutiérrez Ortiz Mena. p. 21

[100] SCJN. Primera Sala. *Amparo en revisión 622/2015*. Aprobado por unanimidad de votos en sesión del 20 de enero de 2016. Ponente: Arturo Zaldívar Lelo de Larrea. De esta sentencia derivó la tesis aislada 1a. CLIII/2016 (10a.) con rubro: PERSONAS Y PUEBLOS INDÍGENAS. SU DERECHO A FUNDAR O UTILIZAR LOS MEDIOS DE COMUNICACIÓN". Registro: 2011773

[101] UNICEF. Derecho a la identidad. La cobertura del registro de nacimiento en México. 2018. Pág, 18. Disponible en: https://www.unicef.org/mexico/media/1016/file/UNICEF_Derecho%20a%20la%20identidad.pdf

pública, por lo que debe reconocerse el incumplimiento del requisito de proporcionalidad y considerar inconstitucionales las normas combatidas al ser violatorias de los artículos 1, 2, 6, 7, 14 y 16 de la CPEUM, 1.1, 13, 24 de la CADH, 2, 19 y 26 del PIDCP.

TERCERO. LA OPERACIÓN DEL PANAUT PRODUCE UN EFECTO INHIBIDOR EN EL EJERCICIO DEL DERECHO A LA LIBERTAD DE EXPRESIÓN Y COMPROMETE EL DERECHO DE EXPRESIÓN ANÓNIMA VULNERANDO EL ARTÍCULO 6 Y 7 DE LA CPEUM, 13 DE LA CADH Y 19 DEL PIDCP.

Las normas combatidas, al establecer a través del PANAUT una base de datos que pretende vincular, de manera indiscriminada, toda línea de telefonía móvil a la identidad de una persona y permitir el acceso a dicha base por parte de autoridades, sin establecer salvaguardas adecuadas, además de vulnerar el derecho a la privacidad y protección de datos personales, repercute en el derecho a la libertad de expresión al producir un efecto inhibidor en el ejercicio de ese derecho y amenazar el derecho de expresión anónima de manera violatoria de los artículos 6 y 7 de la CPEUM, 13 de la CADH y 19 del PIDCP, como a continuación se desarrolla:

A. El derecho de expresión anónima

La libertad de las personas de formarse una opinión y expresar sus ideas, así como buscar y recibir información, requiere espacios de intimidad y anonimato, libres de amedrentamiento y de represalias provocadas por exigencias de identificación o de revelación de creencias, convicciones fuentes de consulta. Es por ello que organismos y tribunales internacionales de derechos humanos han reiterado que el derecho a la privacidad y el derecho a la libertad de expresión se encuentran íntimamente ligados y que de esa estrecha relación se desprende el derecho de expresión anónima[102].

El anonimato y la expresión anónima han jugado un papel fundamental en la historia de la humanidad[103][104] en tanto le han ofrecido a las personas una protección indispensable frente a posibles represalias del Estado, sus empleadores y otros integrantes de la sociedad, al difundir, recibir o buscar información, por ejemplo, que revela abusos de poder, denuncia injusticias o que podría poner en riesgo la vida o integridad física de fuentes periodísticas o de personas defensoras de derechos humanos. Es por ello que la Suprema Corte de los Estados Unidos ha reconocido, en el caso *McIntyre v. Ohio Elections Comm'n*[105], que el anonimato "constituye una tradición honorable de activismo y disenso" que representa además "un escudo frente a la tiranía de la mayoría".

---

[102] CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II.; ONU. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión Frank La Rue. 17 de abril de 2013. A/HRC/23/40, párr. 24; OACNUDH. El derecho a la privacidad en la era digital. 30 de Junio de 2014. A/HRC/27/37; ONU. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión David Kaye. 22 de mayo de 2015. A/HRC/29/32; y TEDH. *Caso "Rotaru vs. Rumania"* Aplicación No. 28341/95. Sentencia del 04 de mayo de 2000. Párr. 42

[103] Jason A. Martin & Anthony L. Fargo, Anonymity as a Legal Right: Where and Why It Matters, 16 N.C. J.L. & Tech. 311 (2015). Disponible en: http://scholarship.law.unc.edu/ncjolt/vol16/iss2/3

[104] Suprema Corte de los Estados Unidos. *Talley v. California*, 362 U.S. 60 (1960), pág. 64-65.

[105] Suprema Corte de los Estados Unidos. *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995), pág. 357.

Esta tradición democrática de reconocimiento y protección al anonimato ha adquirido una importante vigencia con la proliferación de tecnologías digitales la cual ofrece nuevas herramientas para proteger las expresiones anónimas, al mismo tiempo que representa nuevos riesgos de monitoreo y vigilancia[106]. Por esa razón, organismos y tribunales internacionales de derechos humanos han destacado la importancia de la protección del derecho de expresión anónima a través de las TIC.

Por ejemplo, la Oficina de la Alta Comisionada para los Derechos Humanos de la ONU en su informe "***El derecho a la privacidad en la era digital***"[107]; el Relator para la Libertad de Expresión y Opinión de la ONU en su "***Informe sobre la utilización del cifrado y el anonimato en las comunicaciones digitales***"[108]; y la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos en su informe "***Libertad de Expresión e Internet***"[109] coinciden en considerar que el Estado posee la obligación de proteger y no amenazar el derecho al anonimato en línea, estableciendo reglas estrictas para su restricción, a la luz de los principios de necesidad y proporcionalidad.

En concreto, se ha resaltado que medidas que tengan un efecto generalizado e indiscriminado de amenaza al anonimato no son compatibles con el principio de proporcionalidad[110], sino que, en su caso, cualquier medida que pretenda identificar a una persona usuaria de las TIC debe ser focalizada y ser autorizada exclusivamente en sede judicial[111].

En atención de lo anterior, organismos internacionales de derechos humanos han reconocido que requisitos de registro de datos personales de identificación al activar una tarjeta SIM, como es el caso del PANAUT, "**menoscaban directamente el anonimato**, en particular para aquellas personas que acceden a Internet únicamente a través de la tecnología móvil"[112], en tanto dicho registro obligatorio de las tarjetas SIM "puede proporcionar a los gobiernos la capacidad de vigilar a personas y periodistas más allá de cualquier interés gubernamental legítimo"[113].

En efecto, la vinculación de la identidad de las personas a las líneas de telefonía móvil permite conocer una gran cantidad de información sobre una persona debido a la posibilidad de correlacionar y desanonimizar otras bases de datos de las que pueden

---

[106] ONU. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión Frank La Rue*. 17 de abril de 2013. A/HRC/23/40, párr. 11.
[107] OACNUDH. *El derecho a la privacidad en la era digital*. 30 de Junio de 2014. A/HRC/27/37, párr. 20.
[108] ONU. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión David Kaye*. 22 de mayo de 2015. A/HRC/29/32.
[109] CIDH. Relatoría Especial para la Libertad de Expresión. *Libertad de Expresión e Internet*. 31 de diciembre de 2013. OEA/Ser.L/V/II., párrs. 131-136.
[110] OACNUDH. *El derecho a la privacidad en la era digital*. 30 de Junio de 2014. A/HRC/27/37, párr. 20; CIDH. Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013. OEA/Ser.L/V/II., párrs. 136.
[111] CIDH. Relatoría Especial para la Libertad de Expresión. *Libertad de Expresión e Internet*. 31 de diciembre de 2013. OEA/Ser.L/V/II., párrs. 109 y 135.
[112] ONU. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión David Kaye*. 22 de mayo de 2015. A/HRC/29/32, párr. 51.
[113] Ídem.

desprenderse datos como historial de localización, actividades en línea, comunicaciones y relaciones personales, entre muchas otras. Por ello, el Relator Especial de la ONU para la Libertad de Expresión ha concluído que "los Estados **deben abstenerse de establecer la identificación de los usuarios como condición para acceder a las comunicaciones digitales y a los servicios en línea, y de obligar a los usuarios de teléfonos móviles que registren su tarjeta SIM**"[114].

B. Aplicación del parámetro de regularidad constitucional

A la luz de los estándares desarrollados anteriormente, resulta necesario analizar si las interferencias con el derecho a la libertad de expresión, en particular el derecho a la expresión anónima, que provocan las normas combatidas, cumple con los requisitos de idoneidad, necesidad y proporcionalidad.

En este sentido, se reiteran las consideraciones en torno al incumplimiento de los requisitos de **idoneidad y necesidad** expresadas en los conceptos de invalidez precedentes, en tanto resultan idénticamente aplicables por lo que **debe concluirse de igual manera la inconstitucionalidad de las normas combatidas**.

No obstante lo anterior, respecto de la grada de **proporcionalidad**, debe apreciarse en primer lugar que las interferencias con el derecho a la libertad de expresión, en particular al derecho de expresión anónima son de una intensidad alta, derivado de que el requisito de registro obligatorio es masivo e indiscriminado respecto de la totalidad de las personas usuarias de telefonía móvil.

Además, la ausencia de salvaguardas adecuadas, en particular el control judicial, respecto del acceso a la base de datos por parte de autoridades de seguridad y procuración de justicia, intensifica el nivel de las interferencias en el derecho de expresión anónima y producen un efecto inhibidor en el ejercicio de la libertad de expresión, con un impacto particularmente intenso respecto de algunos grupos de población como las personas periodistas, las personas alertadoras de hechos de corrupción y violaciones a derechos humanos, así como a las personas defensoras de derechos humanos.

Como ha sido establecido, el PANAUT, puede permitir a autoridades y otras personas que accedan a la base de datos de manera ilegal, el conocer no solo la posible identidad de los titulares de una línea telefónica, sino cualquier otra información que se encuentre ligada a su número telefónico, lo cual potencialmente permite conocer un gran cúmulo de información de una persona, lo cual facilita medidas de vigilancia masiva que transgreden los principios democráticos.

De esta manera, dado que como ha sido establecido, existe una ausencia absoluta o significativa de contribución al fin perseguido por las medidas contempladas en las normas combatidas, derivada de la ausencia de evidencia de que requisitos de identidad para la adquisición y uso de tarjetas SIM contribuyan a la reducción de índices delictivos, la imposibilidad de presumir que la persona registrada en el PANAUT es la responsable de

[114] Ibídem, párr. 60.

una comunicación y dado que existen múltiples maneras en las que este puede eludirse, como fue desarrollado en el concepto de invalidez primero, es claro que las normas combatidas restringen de manera desproporcionada el derecho a la expresión anónima y generan un efecto inhibidor en el ejercicio del derecho a la libertad de expresión que implica el incumplimiento del requisito de proporcionalidad.

Por lo tanto, debe concluirse que las normas combatidas vulneran el derecho a la libertad de expresión, en particular el derecho de expresión anónima reconocido en los artículos 6 y 7 de la CPEUM, 13 de la CADH y 19 del PIDCP.

CUARTO. EL PÁRRAFO SEGUNDO DEL ARTÍCULO 180 BIS DE LA LFTR VIOLA EL DERECHO A LA PRESUNCIÓN DE INOCENCIA ESTABLECIDO EN EL ARTÍCULO 20, APARTADO A y B DE LA CPEUM, 8 DE LA CADH Y 14.2 DEL PIDCP.

El párrafo segundo del artículo 180 Bis del Decreto combatido establece lo siguiente:

> ***Artículo 180 bis.*** *(...) El registro del número de una línea telefónica móvil en el Padrón Nacional de Usuarios de Telefonía Móvil* ***presume****, con independencia de lo previsto en las leyes aplicables,* ***la existencia de la misma, su pertenencia a la persona que aparece en aquél como titular o propietaria,*** *así como la validez de los actos jurídicos que se relacionan con el respectivo contrato de prestación de servicios en sus diferentes modalidades y que obran en el padrón* ***salvo prueba en contrario, de conformidad con lo establecido en el artículo 20, apartado B fracción I*** *de la Constitución Política de los Estados Unidos Mexicanos y la****s demás disposiciones jurídicas aplicables.***

En otras palabras, este artículo señala las siguientes presunciones derivadas del registro de un número en el Padrón:

1. La existencia de la línea registrada.
2. La persona que aparece como titular en el registro es el propietario de la línea.
3. La validez de los actos jurídicos que se relacionan con el contrato de prestación.

Lo anterior se presumirá como cierto salvo prueba en contrario aunque contradictoriamente, la norma haga referencia a lo establecido en la fracción I del apartado B del artículo 20 constitucional. Dicha fracción establece lo siguiente:

> ***Artículo 20.*** *(...)*
>
> *B. De los derechos de toda persona imputada:*
>
> *I. A que se presuma su inocencia mientras no se declare su responsabilidad mediante sentencia emitida por el juez de la causa;*

Con independencia de la referencia al artículo 20, Apartado B, fracción I de la CPEUM, esta parte quejosa considera que dicho precepto constitucional es vulnerado por el artículo 180

Bis de la LFTR. Para demostrar esto, se hará un breve recuento sobre el contenido del derecho a la presunción de inocencia conforme se ha interpretado en la SCJN y en la Corte IDH. Posteriormente, se comprobará cómo la disposición normativa combatida no cumple con los estándares mínimos expuestos por la jurisprudencia nacional e internacional.

A. Contenido del derecho a la presunción de inocencia

El principio de presunción de inocencia es un principio que trasciende la órbita del debido proceso. La Segunda Sala de la Suprema Corte de Justicia de la Nación, al resolver el ***Amparo en Revisión 89/2007***[115], delineó el contenido de la presunción de inocencia como derecho humano, bajo los siguientes términos:

1. En materia procesal penal, impone la obligación de arrojar la carga de la prueba al acusador.
2. Es un derecho humano que la Constitución reconoce y garantiza en general.
3. Tiene un alcance que trasciende la órbita del debido proceso.
4. Garantiza la protección de otros derechos humanos, como son la dignidad humana, la libertad, la honra y el buen nombre.
5. Opera en situaciones extraprocesales y constituye el derecho a recibir la consideración y el trato de "no autor o no partícipe" de un hecho de carácter delictivo o en otro tipo de infracciones mientras no se demuestra la culpabilidad.

Asimismo, la SCJN ha reconocido en su jurisprudencia que la presunción de inocencia es un derecho universal y continuo, por lo que se goza desde la etapa previa al proceso y se conserva durante la secuela procesal hasta que se dicte sentencia[116], que se encuentra formulado por la Constitución Política de los Estados Unidos Mexicanos y los Tratados Internacionales de los que el Estado mexicano forma parte, como se desprende de los artículos 1° y 20 constitucionales; así como 13 del Código Nacional de Procedimientos Penales.

A su vez, el Comité de Derechos Humanos en su ***Observación General No. 32***[117] sobre el párrafo segundo del artículo 14, ha reconocido tres dimensiones del derecho de presunción de inocencia:

1. El derecho humano de las personas a la presunción de inocencia, siempre y cuando no se demuestre lo contrario.
2. La Imposición de la carga de la prueba al acusador; y

---

[115] SCJN. Segunda Sala. *Amparo en Revisión 89/2007*. Aprobado por unanimidad de votos en sesión del 21 de marzo de 2007. Ponente: Genaro Góngora Pimentel.

[116] Semanario Judicial de la Federación y su Gaceta. Primera Sala. "PRESUNCIÓN DE INOCENCIA EL PRINCIPIO RELATIVO ESTÁ CONSIGNADO EXPRESAMENTE EN LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, A PARTIR DE LA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 18 DE JUNIO DE 2008". Tesis: 1a. I/2012 (10a.) Rubro: 2000124.

[117] Comité de Derechos Humanos. *"Observación General 32: Artículo 14. El derecho a un juicio imparcial y a la igualdad ante los tribunales y cortes de justicia"*. CCPR/C/GC/32. 23 de agosto de 2007. Disponible en: https://undocs.org/es/CCPR/C/GC/32

3. La garantía de que no se presuma la culpabilidad a menos que sea demostrado la acusación, fuera de toda duda razonable, es decir, que el acusado tenga el beneficio de la duda.

La Primera Sala de la SCJN ha reconocido, además, que el derecho a la presunción de inocencia es un derecho poliédrico[118]; en el sentido de que tiene múltiples manifestaciones o vertientes cuyo contenido se encuentra asociado con garantías encaminadas a disciplinar distintos aspectos del proceso penal. Al resolver el ***Amparo en Revisión 349/2012*** se retomó ese criterio explicando que en la dimensión procesal de la presunción de inocencia pueden identificarse al menos tres vertientes del derecho[119]:

1. Regla de trato procesal:
2. Regla probatoria
3. Estándar probatorio.

La modalidad de presunción de inocencia como regla probatoria ha sido definida por la Primera Sala[120] de la SCJN como la regla que "establece los requisitos que debe cumplir la actividad probatoria y las características que debe reunir cada uno de los medios de prueba aportados por el Ministerio Público para poder considerar que existe prueba de cargo válida y destruir así el estatus de inocente que tiene todo procesado".

Es en este mismo Amparo en Revisión 349/2012 se especifica que esta modalidad de la presunción de inocencia contiene de manera implícita la regla que impone la carga de la prueba, norma que determina a qué parte le corresponde aportar las pruebas de cargo. Por lo cual, uno de los requisitos para que una prueba de cargo sea válida es que sea suministradas por la parte que tiene la carga procesal de probar. Esto se reiteró en el ***Amparo Directo en Revisión 3623/2014***[121], donde coincide con que este requisito para la prueba de cargo se desprende de la redacción del artículo 20, apartado a, fracción V y en principio el segundo párrafo del artículo 21 donde la constitución le asigna la parte acusadora al Ministerio Público.

Asimismo, es importante recalcar los criterios de la Corte IDH que retomó la SCJN en el ***Amparo Directo en Revisión 3623/2014***, como lo es la sentencia de ***Ricardo Canese vs Paraguay***. En dicha sentencia, la Corte IDH define que "la presunción de inocencia es un derecho que implica que el acusado no debe demostrar que no se ha cometido el delito que se le atribuye, ya que el onus probandi corresponde a quien le acusa".[122]

---

[118]SCJN Primera Sala. *Amparo en revisión 466/201*1. Aprobado por mayoría de votos en sesión del 9 de noviembre del 2011. Ponente: Arturo Zaldívar Lelo de Larrea.

[119] SCJN. Primera Sala. *Amparo en revisión 349/2012*. Aprobado por unanimidad de votos en sesión del 26 de septiembre de 2012. Ponente: Arturo Zaldívar Lelo de Larrea. p.18.

[120] SCJN. Primera Sala. *Amparo en revisión 349/2012*. Aprobado por unanimidad de votos en sesión del 26 de septiembre de 2012. Ponente: Arturo Zaldívar Lelo de Larrea. p.19. De esta sentencia y resoluciones subsecuentes derivó la tesis jurisprudencial 1a./J. 25/2014 (10a.) con el rubro: "PRESUNCIÓN DE INOCENCIA COMO REGLA PROBATORIA**".** Registro: 2006093.

[121] SCJN. Primera Sala. *Amparo Directo en Revisión 3626/2014*. Aprobado por mayoría de votos en sesión del 26 de agosto de 2015. Ponente: Arturo Zaldívar Lelo de Larrea. p. 41

[122] Corte IDH. *Caso Ricardo Canese vs Paraguay*. Sentencia 31 de agosto de 2004. párr. 154

La CPEUM, la SCJN y la Corte IDH concuerdan que un requisito indispensable de la presunción de inocencia es que la carga probatoria recaiga sobre el Ministero Público y no el acusado. Por lo cual, una disposición que revierta la carga de la prueba sobre el acusado debe de considerarse como violatoria al derecho a la presunción de inocencia.

B. La inconstitucionalidad del artículo 180 Bis de la LFTR al violar el derecho a la presunción de inocencia en su modalidad de regla probatoria.

La presunción establecida señala que la persona registrada como titular de la línea es dueña de la línea de telefonía móvil. Esta presunción revierte de la carga de la prueba de manera injustificada hacia las y los ciudadanos.

El artículo 180 Bis de la LFTR ignora la jurisprudencia nacional e internacional respecto a la presunción de inocencia e impone una carga probatoria excesiva sobre las y los ciudadanos. Esto es así pues la presunción implica que las personas que aparezcan como titulares tengan que probar un hecho negativo: a saber, que no son el titular, que ellos no usan la línea o que alguien más hizo mal uso de la misma.

No se puede omitir que el legislador pensó este artículo bajo el fin de perseguir delitos de extorsión o relacionados con crimen organizado, por lo cual, es claro que el precepto impugnado busca que esta presunción sea utilizada como prueba de cargo contra las personas titulares de la línea en caso de que se haya cometido un hecho delictivo con ese número telefónico. Este es otro motivo por el cual este precepto normativo viola la presunción de inocencia, pues remueve uno de los requisitos más importantes de la modalidad de regla probatoria al deslindar a la parte acusadora de investigar y presentar una de las pruebas de cargo más relevantes para poder enervar la presunción de inocencia.

Inclusive, si pretendiera argumentarse que la referencia al artículo 20, apartado B, fracción I de la CPEUM demuestra la compatibilidad del artículo 180 Bis de la LFTR con el principio de presunción de inocencia, debe señalarse que el uso de este precepto constitucional como máxima interpretativa, además de no evitar las violaciones al principio en la práctica, es inexacto y, de hecho, vulnera el propio derecho a la presunción de inocencia.

Esto es así en virtud de que si bien la fracción I del apartado B del artículo 20 de la Constitución se refiere a la presunción de inocencia del imputado, esta fracción remite a la modalidad de este derecho como regla de tratamiento procesal, mientras que la fracción V del mismo artículo recoge la garantía que otorga a la parte acusadora la carga de la prueba. Por consecuencia, es claro que el artículo 180 Bis de la LFTR contraviene una garantía esencial para la presunción de inocencia reconocida dentro del texto constitucional, como es la obligación que tiene el Ministerio Público de aportar las pruebas de cargo. Todo esto deriva en la indefensión probatoria, la inseguridad jurídica y la violación del derecho a la presunción de inocencia de las y los ciudadanos.

En conclusión, **el artículo 180 Bis debe ser declarado inconstitucional por violentar el principio de presunción de inocencia en su modalidad de regla probatoria contenida**

en la fracción V del artículo 20 constitucional. Esto pues revierte la carga de la prueba de manera excesiva sobre las y los ciudadanos, exenta a la parte acusadora de investigar y presentar pruebas de cargo y señala de manera errónea la fracción I del apartado b del artículo 20 de la CPEUM como único principio de interpretación de dicha norma.

III. PETITORIOS

En vista de los argumentos expuestos y fundados en este escrito, se solicita a esta H. SCJN:

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

SEGUNDO.- En su oportunidad, resuelva como procedentes y fundadas las acciones de inconstitucionalidad 82/2021 y su acumulada 86/2021.

PROTESTO LO NECESARIO, en la Ciudad de México a los tres días del mes de febrero del año dos mil veintidós.

LUIS FERNANDO GARCÍA MUÑOZ
RED EN DEFENSA DE LOS DERECHOS DIGITALES (R3D)

ORGANIZACIONES FIRMANTES

- **ACCESS NOW - Internacional**
- **ARTICLE 19, Oficina para México y Centroamérica**
- **ASOCIACIÓN POR LOS DERECHOS CIVILES (ADC) - Argentina**
- **ASOCIACIÓN TEDIC - Paraguay**
- **DERECHOS DIGITALES - América Latina**
- **FUNDACIÓN INTERNETBOLIVIA.ORG - Bolivia**
- **FUNDACIÓN KARISMA - Colombia**
- **HIPERDERECHO - Perú**
- **INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR (IDEC) - Brasil**
- **OBSERVATEL A.C. - México**
- **PRIVACY INTERNATIONAL - Internacional**
- **RED EN DEFENSA DE LOS DERECHOS DIGITALES (R3D) - México**
- **REDES POR LA DIVERSIDAD, EQUIDAD Y SUSTENTABILIDAD A.C. (REDES AC)**