Ilustre y Nacional
Colegio de Abogados de México
Fundado en 1760

Amicus Curiae

Ilustre y Nacional Colegio de Abogados de México

Ciudad de México a 3 de septiembre de 2021

AMICUS CURIAE

Presentado ante la

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN

con motivo de la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021 y los Recursos de Reclamación 56/2021-CA y 57/2021-CA promovidos por diversos Senadores de la República, integrantes de la LXIV Legislatura y por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Índice

Amicus Curiae

I. Introducción[1]

El Ilustre y Nacional Colegio de Abogados de México (en adelante "INCAM" y/o "el Colegio") tiene una bicentenaria tradición de ser una casa abierta al estudio del Derecho y preocupada por la excelencia de la profesión. Sus ideales, se encuentran consagrados en un Código de Ética Profesional y sus estatutos. Desde su fundación en 1760, el INCAM se ha caracterizado por su fuerte compromiso con la defensa de los derechos de la sociedad mexicana y ha fungido como un órgano de permanente consulta, análisis y asesoramiento de los poderes ejecutivo, legislativo y judicial mediante la emisión de pronunciamientos particulares sobre acontecimientos jurídicos relevantes para la sociedad y comunidad jurídica en general.

La formulación de este Amicus Curiae responde al firme compromiso del Colegio por la defensa y difusión de los derechos humanos en México. El INCAM, a través de su Observatorio de Derechos Humanos (en adelante "Observatorio") ha elaborado el presente documento con el ánimo de colaborar activamente con la Suprema Corte de Justicia de la Nación en el análisis y resolución de la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021 promovidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante "INAI") y por diversos Senadores de la República, integrantes de la LXIV Legislatura (en adelante "los Senadores de la LXIV Legislatura") así como en la de los Recursos de Reclamación 56/2021-CA y 57/2021-CA promovidos por los mencionados sujetos legitimados.

De esta forma, en este documento se realiza un análisis del contenido de los argumentos formulados por el INAI y los Senadores de la LXIV Legislatura en la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021 así como una exposición de pronunciamientos particulares que este Colegio remite a ese H. Máximo Tribunal por conducto de este documento.

Finalmente, se realiza un pronunciamiento particular sobre los Recursos de Reclamación 56/2021-CA y 57/2021-CA con el propósito de que ese Máximo Tribunal los considere para el análisis de los referidos recursos.

II. Justificación

[1] Agradecemos ampliamente al equipo que elaboró este escrito, conformado por Gregorio Barco Vega, Alexis Cervantes Padilla, Isabel Davara F. De Marcos y José Ernesto Rodríguez Duque, con la coordinación y apoyo de Valentina Fix Martínez.

El INCAM a través de su Observatorio de Derechos Humanos como organización comprometida con la defensa y promoción de los derechos humanos ha identificado la publicación del Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión y que, entre otras cosas, establece la creación de un Padrón Nacional de Usuarios de Telefonía (en adelante "PANAUT") publicado el 16 de abril de 2021 en el Diario Oficial de la Federación (en adelante "el Decreto" y/o la norma general impugnada) como una medida regresiva y violatoria de diversos derechos humanos previstos en la Constitución Política de los Estados Unidos Mexicanos (en adelante "Constitución" o "CPEUM") teniendo un alto impacto y consecuencias jurídicas en la defensa efectivo de los derecho humanos de las personas en México.

En este sentido, el INCAM, por conducto de su Observatorio, busca pronunciarse ante la SCJN con el propósito de fortalecer los argumentos que permitan la protección de los derechos humanos de las personas que se ven afectadas a partir de la publicación del Decreto, motivo por el cual este Organismo presenta ante ese Máximo Tribunal el presente Amicus Curiae, en el que se expondrán distintos argumentos legales con la finalidad de fortalecer las manifestaciones realizadas por el INAI y los Senadores de la LXIV Legislatura en relación con la validez del Decreto que reforma la Ley Federal de Telecomunicaciones y Radiodifusión (en adelante "LFTR") evidenciando la inconstitucionalidad de los preceptos del Decreto, por ser contrarios a lo establecido en los artículos 1o, 6o, segundo y tercer párrafos; apartado A, fracciones II, III y VIII, párrafos primero y segundo, 14, 16, 28, 73, fracciones XXIX-O y XXIX-S; y, 133 de la Constitución Federal; 11 de la Convención Americana de Derechos Humanos (en adelante "CADH"); 17 del Pacto Internacional de Derechos Civiles y Políticos (en adelante "PIDCP"); 12 de la Declaración Universal de Derechos Humanos (en adelante "DUDH"); 5, 7 y 8 del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; 1° de su Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a la Autoridades de Control y a los Flujos Fronterizos de Datos (en adelante "Convenio 108); y, 8 y 16 de la Convención de los Derechos del Niño (en adelante "CDN").

III. Interés del Promovente

El INCAM es una organización sin fines de lucro que, entre sus objetivos, tiene la defensa y promoción de los derechos humanos en México. A través de su Observatorio, el INCAM realiza distintas acciones vinculadas con la promoción y defensa de los derechos humanos en México, entre las que destacan la elaboración y difusión de documentos de análisis legal, el análisis del marco jurídico actual y propuesto en materia de derechos humanos en México y los

distintos sistemas de protección de derechos humanos existentes en el mundo, la elaboración y publicación de documentos y contenidos de interés para la sociedad en redes sociales, la colaboración con diversas organizaciones promotoras de derechos humanos, la formulación de posicionamientos concretos sobre temas que pueden tener algún impacto en los derechos humanos tutelados en la Constitución y tratados de los que México forma parte como el caso del Decreto referido en este documento.

De acuerdo con lo anterior, para el Colegio la resolución de la Acción de Inconstitucionalidad 82/2021, su acumulada 86/2021 y de los Recursos de Reclamación formulados por el INAI y los Senadores de la LXIV Legislatura, puede incidir de forma significativa en los derechos humanos de la sociedad mexicana y que se encuentran reconocidos en la Constitución y diversos instrumentos internacionales de los que México forma parte.

En lo que concierne a la solicitud de suspensión solicitada por los órganos promoventes de la Acción de Inconstitucionalidad 82/2021, su acumulada 86/2021 y de los Recursos de Reclamación, este Colegio considera que el hecho de no conceder la suspensión del Decreto se actualizarían irremediablemente diversas violaciones a los derechos humanos de las personas, concretamente de los derechos a la privacidad, protección de datos personales, acceso a las Tecnologías de la Información y las Comunicaciones (TIC), legalidad, presunción de inocencia, derecho al trabajo, competencia económica, derechos de la niñez, entre otros.

En tal virtud, por conducto de este documento se presentan las consideraciones de derecho para demostrar la procedencia de los argumentos hechos valer por el INAI y los Senadores de la LXIV Legislatura en la Acción de Inconstitucionalidad 82/2021, su acumulada 86/2021 y de los correspondientes Recursos de Reclamación.

IV. Objetivo

El objetivo del Amicus Curiae es proporcionar a los ministros de la SCJN argumentos de hecho y de derecho, con perspectiva de derechos humanos, que evidencian la inconstitucionalidad del Decreto. Esto con motivo de la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021, promovidas por el INAI y los Senadores de la LXIV Legislatura.

En razón de lo anterior, se analizarán los conceptos de invalidez hechos valer por cada uno de los órganos legitimados referidos en la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021.

En este contexto, es importante señalar que el presente Amicus Curiae se presenta con el ánimo de aportar elementos para el análisis de fondo de las acciones de inconstitucionalidad, pues, la sentencia que se dicte, puede impactar significativamente en el ejercicio de los derechos humanos de todas aquellas personas que son usuarias de una línea telefónica celular en México; es por ello que en su contenido se pide respetuosamente a esa SCJN reconocer la invalidez del Decreto impugnado en la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021, promovidas por el INAI y los Senadores de la LXIV Legislatura.

Con los elementos aportados, se pretende contribuir al análisis que realice la SCJN sobre la constitucionalidad del Decreto, ya que, como se observará en el contenido del presente documento, la emisión del citado Decreto impacta sustancialmente en los derechos humanos de privacidad, protección de datos personales, acceso a las Tecnologías de la Información y las Comunicaciones (TIC), legalidad, presunción de inocencia, derecho al trabajo, competencia económica, derechos de la niñez reconocidos en la Constitución y diversos instrumentos internacionales de los que México forma parte.

V. Antecedentes

Como antecedentes del Decreto se pueden señalar los siguientes:

1. El 5 de diciembre de 2019, el diputado Mario Delgado y el Grupo Parlamentario de MORENA presentaron una iniciativa para adicionar y reformar la Ley Federal de Telecomunicaciones y Radiodifusión. Esta iniciativa dio inicio al proceso legislativo y fue turnada a la Comisión de Comunicaciones y Transportes.
2. Posteriormente, se presentaron otras iniciativas y para el día 10 de diciembre fue aprobado por Pleno de la Cámara de Diputados, el dictamen correspondiente, con una votación de 392 a favor, 44 en contra y nueve abstenciones. 1
3. El 11 de diciembre de 2020 se remitió al Senado la minuta correspondiente, siendo turnada la misma el día 15 a las Comisiones Unidas de Comunicaciones y Transportes y de Estudios Legislativos. El proyecto de dictamen fue aprobado en el Pleno el 13 de abril de 2021 con 54 votos a favor, 49 en contra y 10 abstenciones.
4. Finalmente, el 16 de abril de 2021 fue publicado en el Diario Oficial de la Federación (en adelante “DOF”) el Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión (“Decreto”).

5. El 13 de mayo de 2021 el INAI presentó ante el Pleno de la SCJN la demanda acción de inconstitucionalidad en contra del Decreto.
6. El 25 de mayo de 2021 los Senadores de la LXIV Legislatura presentaron ante el Pleno de la SCJN la demanda acción de inconstitucionalidad en contra del Decreto.
7. En un acuerdo publicado el 27 de mayo de 2021, ese H. máximo tribunal informó sobre el proceso de las acciones de inconstitucionalidad 82/2021y 86/2021, promovidas respectivamente por el INAI y por los Senadores de la LXIV Legislatura.
8. El 11 de junio de 2021 los Senadores de la LXIV Legislatura presentaron ante la SCJN el Recurso de Reclamación 56/2021-CA en contra del proveído de 27 de mayo de 2021, dictado por la Ministra Instructora Norma Lucía Piña Hernández, en la Acción de Inconstitucionalidad 82/2021 y su acumulado 86/2021, en el que se negó la suspensión respecto de la norma general impugnada.
9. El 17 de junio de 2021 el INAI presentó ante la SCJN el Recurso de Reclamación 57/2021-CA en contra del proveído de 27 de mayo de 2021, dictado por la Ministra Instructora Norma Lucía Piña Hernández, en la Acción de Inconstitucionalidad 82/2021 y su acumulado 86/2021, en el que se negó la suspensión respecto de la norma general impugnada.

VI. Argumentos relacionados con los conceptos de invalidez hechos valer por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

En la acción de inconstitucionalidad 82/2021 interpuesta ante ese Máximo Tribunal el pasado 13 de mayo de 2021, el INAI reclamó la validez del Decreto, en particular, de sus artículos 15, fracción XLII Bis, 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), 180 Sextos, 180 Septimus, 190, fracciones VI y VII, 307 Bis, 307 Ter, 307 Quáter, 307 Quintus, Primero, Segundo, Tercero, Cuarto, Quinto y Sexto, todos Transitorios del mismo Decreto.

Como preceptos del parámetro de regularidad constitucional que se estiman violados el INAI consideró los siguientes: Los artículos 1o, 6o, segundo y tercer párrafos; apartado A, fracciones II, III y VIII, párrafos primero y segundo, 14, 16, 28, 73, fracciones XXIX-O y XXIX-S; y, 133 de la CPEUM; 11 de la CADH; 17 del PIDCP; 12 de la DUDH; 5, 7 y 8 del Convenio 108; 1° de su Protocolo Adicional y, 8 y 16 de la CDN.

En relación con lo anterior, se describen los diversos conceptos de invalidez hechos valer por el INAI y los en la acción de inconstitucionalidad 82/2021 el INAI hace valer los siguientes conceptos de invalidez.

1. Primer concepto de invalidez

Como primer concepto de invalidez el INAI indica los artículos 15, fracción XLII bis, 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes, 180 Sextus, 180 Septimus, Primero, Cuarto y Quinto Transitorios del Decreto impugnado, al establecer la creación del PANAUT, que contendrá información y datos personales de las personas, son violatorios de los derechos relativos a la privacidad, la protección de los datos personales, interés superior del menor y derecho a la identidad, contenidos en los diversos 6o, Apartado A, fracción II, y 16 constitucionales, 11 de la CADH 17 del PIDCP, 12 de la DUDH, V de la DADH y 8 y 16 de la CDN.

Derivado de esto, en su primer concepto de invalidez el INAI sostiene que, el sistema normativo establecido en los artículos impugnados, viola los derechos de privacidad, intimidad, protección de los datos personales, interés superior del menor e identidad, dado que intervienen de forma arbitraria en el ámbito más privado e íntimo de las personas, sin tomar en consideración que todas las personas gozan de un espacio de proyección de su existencia que quede reservado de la invasión y la mirada de los demás, incluso del Estado, pues en esta área es que se desarrolla plenamente la personalidad. Para demostrar las vulneraciones a cada derecho, es necesario acudir al alcance de cada uno, para posteriormente analizarlo frente a la reforma a la LFTR el INAI realiza un análisis de los distintos derechos en juego y señala lo siguiente:

- **En relación con el derecho a la privacidad.** El INAI señala que “El derecho a la privacidad permite a las personas mantener fuera del conocimiento de los demás o dentro del círculo de las personas más próximas ciertas manifestaciones o dimensiones de su existencia (conducta, datos, información, objetos) y la correspondiente obligación de los demás de que no las invadan sin su consentimiento y señala las siguientes premisas:
    - La CPEUM y los tratados internacionales reconocen el derecho de toda persona a la vida privada;
    - El derecho a la vida privada origina la posibilidad de las personas a mantener fuera del conocimiento de los demás (incluidas las autoridades) ciertas manifestaciones o dimensiones de su existencia (conducta, datos, información, objetos) y la correspondiente obligación de que los demás no las invadan sin su consentimiento;
    - La intimidad es una vertiente deld erecho a la privacidad;
    - El derecho a la intimidad consiste en el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona.

- Asimismo, el derecho a la intimidad significa el poder de decisión sobre la publicidad o información de datos relativos a su persona.

- **En relación con el derecho a la protección de datos personales.** El INAI precisa que el derecho a la protección de los datos personales, como un medio de salvaguarda de otros derechos fundamentales previstos en la propia Constitución y en los tratados internacionales de los que México es Parte, implica el derecho a no ser molestado por terceros en ningún aspecto de su persona, entre los que se encuentra la forma en que se ve a sí mismo y como se proyecta a los demás, así como de aquellos que corresponden a los extremos más personales de la vida y del entorno familiar, o que permiten el desarrollo integral de su personalidad como ser humano. Es en esa medida que el derecho de protección de los datos personales, se relaciona de forma estrecha, a partir de los principios de invisibilidad e interdependencia, con el derecho a la vida privada, honor, intimidad, dignidad humana y otros. En esencia, según INAI, implica que las personas tienen el poder de disposición y control sobre sus propios datos, lo que se denomina autodeterminación informativa. Además precisa lo siguiente:
  - Los motivos fundamentales que el Poder Reformador de la Constitución tuvo para proteger de manera directa los datos personales fueron, por un lado, dotar a las personas del poder de disposición y control sobre los datos que les conciernan y, por el otro, avanzar a la par que la sociedad y la tecnología, pues sus adelantos han generado nuevos riesgos para la privacidad de las personas en lo que se ha dado en llamar la “sociedad de la información”. Razón por la cual se protegen esos datos que se emplean en el desenvolvimiento de las comunicaciones e intercambio de información.
  - Se consideran relevantes diversos instrumentos internacionales, como el Convenio 108 y su protocolo, en donde se reconoce como fin, garantizar en el territorio de cada Parte, a cualquier persona física, sean cuales fueren su nacionalidad o su residencia, el respeto a sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (“protección de datos”).
  - La protección a los datos personales, no solamente implica el que las autoridades, como lo establecen los artículos 100 y 116 de la Ley General de Transparencia y Acceso a la Información Pública (en adeñante “LGTAIP”) y 2, fracción V,13 y demás relativos de la Ley General de Protección de Datos Personales en Posesión de Sujetos

Obligados (en adelante “LGPDPPSO”), clasifiquen la información como confidencial y/o que protejan los datos que posean, sino que comprende una temporalidad *ex ante*. Es decir, protege de forma anticipada lo que la autoridad y/o particulares, hagan con esos datos. Esto es, el derecho a la protección de los datos personales no sólo implica que las autoridades protejan todos los datos que tengan en su posesión, sino que también protege un momento previo a esa posesión, esto es, su recopilación o u obtención.

- Las personas tienen el derecho a que se protejan su identidad y sus datos personales, desde su recopilación u obtención. En ese sentido, cualquier acto de autoridad que restrinja o intervenga el derecho a la protección de datos personales, desde su obtención o recopilación, deberá estar plenamente justificada.
- El INAI considera que el Decreto, no se ajusta al marco jurídico vitgente, en tanto vulnera el derecho a la protección de datos personales y la intimidad y privacidad al solicitar una serie de datos que en su conjunto dan una radiografía de la vida privada de las personas.
- El INAI considera que los artículos que se reclaman, ordenan la creación de una base de datos, que obtendrá, recopilará, almacenará, registrará y conservará, los datos personales que se ordenan en el artículo 180 Ter, a saber: número de línea telefónica móvil, fecha y hora de activación de la línea adquirida en la tarjeta SIM, tarjeta SIM, nombre completo o denominación social del usuario o razón social, nacionalidad, número de identificación oficial o clave CURP del titular de la línea, datos biométricos del titular o representante legal de la persona moral, domicilio del usuario, datos del concesionario o de los autorizados.
- El INAI considera que la disposición establecida en el artículo 180 Septimus, que ordena que la información contenida en el PANAUT será confidencial y reservada en términos de la LGTAIP y LGPDPPSO y LFPDPPP, no es suficiente para proteger los datos personales, pues se insiste, la protección constitucional se origina desde su obtención. Esto es así, pues el Estado no tiene la facultad de recabar datos personales de forma indiscriminada, como sucede en el caso concreto, sino que la decisión de obtenerlos, debe estar plenamente justificada en intereses legítimos y ser acordes con el parámetro de regularidad constitucional.
- El INAI considera que término, los artículos reclamados exigen la recopilación, obtención, registro, conservación, almacenamiento, acceso, utilización, comunicación, posesión, manejo y transferencia

de los datos personales, incluidos datos sensibles, lo cual, por sí mismo, es violatorio del derecho a la protección de los datos personales y del derecho a la privacidad e intimidad de las personas, pues vacían de forma absoluta el contenido del derecho, al exponer, sin limitación ni justificación legítima, datos personales que se refieren a todas las personas, a sus atributos y a su identidad.

- El INAI considera que, no se establecen limitaciones o excepciones de ningún tipo, sino que recaba la información de todas las personas sin distingo alguno.
- El INAI considera que la información requerida por los artículos en comento, por sí sola dará una radiografía de la vida privada de las personas, sin una razón legítima. Es decir, esta radiografía implica acceso a la situación patrimonial, económica, de seguridad, integridad de las personas y, en consecuencia, en su privacidad. De tal forma que toda apertura en la protección a estos datos, actualizada desde el momento en que se ordena de su recopilación u obtención, pasando por su registro y almacenamiento, hasta su uso y transferencia, constituyen una violación del derecho de protección a los datos personales y al derecho a la vida privada, consagrados en los artículos 6o, Apartado A, fracción II, y 16, primer y segundo párrafos, constitucionales, y 11 de la CADH, 17 del PIDCP, 12 de la DUDH y V de la DADDH.
- El INAI considera que no sólo se viola el derecho de protección a los datos personales y la privacidad sino que se viola la intimidad de los ciudadanos, ya que dentro de los datos personales existe una categoría que precisamente afecta los aspectos más íntimos16 de las personas, y que se denominan datos personales sensibles, entre los que podemos encontrar los datos biométricos, toda vez que se encuentran dirigidos a identificar de manera unívoca a las personas, además de que pueden dar cuenta del origen racial o étnico, entre otras características.
- El INAI considera que, si los datos personales sensibles, como los datos biométricos, se encuentran protegidos por el derecho a la intimidad, vulnerar la protección a estos datos implicará vulnerar un derecho personalísimo -la intimidad- que protege el contenido más profundo de la privacidad y que debe estar radicalmente vedado.
- Finalmente, El INAI considera que los nuevos artículos incluidos a la LFTR facultan al Instituto Federal de Telecomunicaciones (en adelante “IFT”) a llevar todas las operaciones necesarias para operar, regular y mantener el PANAUT, lo que implica que el IFT en cita será quien trate los datos personales a través del PANAUT.

- El INAI considera que la reforma incluida a la LFTR es contraria a los derechos de privacidad, protección a los datos personales e intimidad, en tanto que, por los datos que se solicitan, se puede permitir el acceso a información que puede tener implicaciones negativas en un sinfín de situaciones personales sin que exista una justificación adecuada de limitación a tales derechos.

- **Derecho a la identidad.** El INAI sostiene que el derecho a la identidad se refiere al conjunto de elementos que construyen la individualidad de una persona. La ausencia de este derecho genera consecuencias negativas en la esfera de cada individuo, en tanto que imposibilitan el ejercicio de otros derechos. De modo que su naturaleza es la de un derecho independiente que identifica a una persona en concreto mediante la suma de distintos factores, pero igualmente funciona como un instrumento que permite ejercer prerrogativas de otra naturaleza. Además, el INAI señala que:
  - La CPEUM, en el artículo 4o reconoce que toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. Así, a juicio de la Primera Sala de la SCJN, la identidad persigue proteger la conformación de la autopercepción como faceta identitaria, aunado a que este concepto no se agota en la parte biológica, sino que se construye a partir de múltiples factores psicológicos y sociales de la manera en la que el individuo se concibe y los rasgos definitorios de su personalidad.
  - El PANAUT será una base de datos alimentada de manera descentralizada, en la que no se advierten mecanismos de protección de datos personales a fin de evitar abusos por parte de las compañías telefónicas, sin perjuicio de que incluso, también existieran otros actores involucrados, como las operadoras móviles virtuales. El derecho a la identidad se quebrantaría desde la óptica de que ni el IFT, ni las empresas telefónicas, podrían asegurar que sus medidas de tratamiento son eficaces para que sus datos personales integren directamente el padrón, sin que en el tramo relativo a su conformación, se lleve un tratamiento contrario a los principios y deberes en materia de protección de datos personales.
  - Por otra parte, el funcionamiento del PANAUT se encuentra redactado de una forma genérica, es decir, transgrediendo el principio de taxatividad normativa, en la que no se prevén las obligaciones mínimas de cuidado para evitar cualquier perdida que origine la suplantación o robo de identidad. Esto es, el marco jurídico establecido en la LFTR, que activa el funcionamiento del padrón, en donde se prevé la obligación de entregar datos biométricos, no es

suficiente y no contiene los controles necesarios para evitar accidentes.

- El INAI recalca que como ejemplo de la falta de controles para asegurar el debido tratamiento, el artículo 180 Quintes considera la posibilidad de recabar los datos biométricos y el domicilio del usuario, a través de medios digitales o medios remotos. Con esta previsión se debilitan aún más el derecho a la identidad, cuya obligación de protegerlo, promoverlo, respetarlo y garantizarlo, recae en cada autoridad del Estado mexicano, incluyendo al IFT, lo cual claramente se incumple.
- En este sentido, el INAI considera que la inexistencia de medidas de cuidado para tratar los datos biométricos que serán incluidos en el PANAUT deriva en peligro latente que transgrede el derecho de identidad de los usuarios de telefonía móvil. Esa amenaza se refuerza por el hecho de que distintos actores tendrán acceso a cada uno de los datos que se entreguen, lo que abre la puerta a conductas ilegítimas que terminen en un robo de identidad.

- **Derechos de la niñez e interés superior del menor**. El INAI recuerda que en el artículo 4o constitucional se reconoce de forma expresa que en todas las decisiones y actuaciones del Estado se velará y cumplirá con el principio del interés superior de la niñez, garantizando de manera plena sus derechos. Del mismo modo, se contempla que los niños y las niñas tienen derecho a la satisfacción de sus necesidades de alimentación, salud, educación y sano esparcimiento para su desarrollo integral. En relación con la violación de estos derechos con motivo del Decreto, el INAI señala lo siguiente:
  - Que la CDN, a lo largo de sus 54 artículos, reconoce que los niños son individuos con derecho de pleno desarrollo físico, mental y social, y con derecho a expresar libremente sus opiniones. Para ello, se reconoce expresamente el derecho a la vida; la inscripción inmediata después del nacimiento; identidad; nacionalidad; nombre; el mantenimiento de relaciones familiares, entre otras obligaciones. En esencia, lo que se exige a los Estados es que en todas las medidas que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, deberán atender de forma primordial al interés superior del menor. Este principio constituye el elemento fundamental que debe servir de guía a las autoridades y particulares para realizar un acto que tenga impacto en la esfera de un niño.
  - Que al tratarse de un derecho que se ubica dentro de la esfera jurídica del integrante de un grupo en situación vulnerabilidad, el

derecho internacional y el derecho interno, exigen que cualquier acto legislativo, administrativo o judicial, debe tener especial cuidado en no transgredir o afectar mínimamente su contenido, pues el efecto que se genera en grupos en situación de vulnerabilidad es mayor al producido en particulares que no pertenecen a éstos.

- Que tanto la normativa nacional como internacional sientan las bases jurídicas para reforzar la protección de los niños y niñas frente a los actos estatales o particulares que les pueden generar un daño irreparable, el cual, se reitera, tiene un impacto mayor en ellos, al ser parte de un grupo en situación de vulnerabilidad. En ese sentido, las autoridades del Estado deben atender a estos parámetros que, sin duda, se encuentran fundados en el principio de interés superior del menor, a fin de crear un ambiente progresivo e integral por lo que respecta a la garantía de sus derechos.
- La LFTR, aun cuando no hace referencia expresa a la entrega de datos biométricos por parte de los niños y niñas, la realidad es que no se hace una distinción entre usuarios móviles, lo que hace presumir que, dentro del universo de sujetos obligados a entregar sus datos personales, entre ellos, los biométricos, se contempla precisamente a los niños y niñas. Esto es, tomando en cuenta que, como se mencionó al inicio de este apartado, la quinta parte de los niños de entre 8 y 12 años poseen un teléfono celular, éstos adquieren el carácter de usuarios móviles que serán objeto de control por parte del Instituto Federal de Telecomunicaciones mediante la instauración del padrón.
- En resumen, el INAI señala que al no realizar una distinción entre usuarios de telefonía, se violan diversos derechos, pero en distintos niveles dependiendo de la edad del usuario. Con ello, se viola sistemáticamente el derecho a la identidad, la privacidad y los datos personales, con lo que se vacía de contenido del interés superior del menor, haciendo prevalecer el interés del Estado en perseguir una finalidad que no es legítima.
- En este sentido, el INAI considera que, al no excluir del padrón a los niños y niñas, se produce una violación automática de los artículos 4o constitucional, 8 y 16 de la CDN; y 7 de la LGPDPPSO, por ello, es necesario declarar la invalidez de los preceptos que son contrarios a los numerales referidos.

En relación con lo anterior, este Colegio coincide plenamente con los argumentos esgrimidos por el máximo órgano garante de la protección de datos personales en que la emisión del Decreto transgrede los derechos humanos a la vida privada,

protección de datos personales, identidad e interés superior del menor por las razones siguientes:

- **<u>En relación con el derecho a la vida privada</u>**. Coincidimos con el INAI en la conceptualización jurídica de este derecho y su relevancia para el ordenamiento jurídico mexicano, por lo que, consideramos es importante que se tome en cuenta que este derecho al estar reconocido en diversos ordenamientos jurídicos nacionales e internacionales se constituye como un derecho humano de todas las personas en México, por lo que, debe ser garantizado y protegido, en particular, cuando se presentan injerencias arbitrarias e injustificadas como lo es la creación del PANAUT, que como se describirá de forma posterior, es una medida desproporcionada y excesiva cuya creación incide directa e injustificadamente en este derecho al no tener una justificación constitucional ni legítima, tal y como lo ha expresado el Instituto al abordar la proporcionalidad de esta medida en relación con el baremo de constitucionalidad y los requisitos de necesidad, idoneidad y proporcionalidad en sentido estricto para decretar la restricción de algún derecho fundamental. En relación con este derecho, insistimos en la relevancia de esta prerrogativa en nuestro ordenamiento jurídico y nos permitimos destacar lo siguiente:
    - El derecho a la *vida privada* "es un derecho de la personalidad que protege a las personas de no ser interferidos en aquellas actividades que se reservan al ámbito personal y que se excluyen del escrutinio de la actividad pública". Así, este concepto se ha relacionado con lo que no constituye vida pública; el ámbito reservado frente a la acción y el conocimiento de los demás; lo que se desea compartir únicamente con aquellos que uno elige; las actividades de las personas en la esfera particular, relacionadas con el hogar y la familia; o aquello que las personas no desempeñan con el carácter de servidores públicos.[2]

[2] DERECHO A LA VIDA PRIVADA. SU CONTENIDO GENERAL Y LA IMPORTANCIA DE NO DESCONTEXTUALIZAR LAS REFERENCIAS A LA MISMA.
La Suprema Corte de Justicia de la Nación se ha referido en varias tesis a los rasgos característicos de la noción de lo "privado". Así, lo ha relacionado con: lo que no constituye vida pública; el ámbito reservado frente a la acción y el conocimiento de los demás; lo que se desea compartir únicamente con aquellos que uno elige; las actividades de las personas en la esfera particular, relacionadas con el hogar y la familia; o aquello que las personas no desempeñan con el carácter de servidores públicos. Por otro lado, el derecho a la vida privada (o intimidad) está reconocido y protegido en declaraciones y tratados de derechos humanos que forman parte del orden jurídico mexicano, como la Declaración Universal de los Derechos Humanos (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos (artículo 17), la Convención Americana sobre Derechos Humanos (artículo 11) y la Convención sobre los Derechos del Niño (artículo 16). Al interpretar estas disposiciones, los organismos internacionales han destacado que la noción de vida privada atañe a la esfera de la vida en la que las personas pueden expresar libremente su identidad, ya sea en sus relaciones con los demás o en lo individual, y han destacado su vinculación con un amplio abanico de otros derechos, como la inviolabilidad de la correspondencia y de las comunicaciones en general, la inviolabilidad del domicilio, las garantías respecto de los registros personales y corporales, las relacionadas con la recopilación y registro de información personal en bancos de datos y otros dispositivos; el derecho a una vivienda adecuada, a la salud y a la igualdad; los derechos reproductivos, o la protección en caso de desalojos forzados. Las afirmaciones contenidas en las resoluciones nacionales e internacionales son útiles en la medida en que no se tomen de manera descontextualizada, emerjan de un análisis cuidadoso de los diferentes escenarios jurídicos en los que la idea de privacidad entra en juego y no se pretenda derivar de ellas un concepto mecánico de vida privada, de referentes fijos e inmutables. Lo único que estas resoluciones permiten reconstruir, en términos abstractos, es la imagen general que evoca la idea de privacidad en nuestro contexto cultural. Según esta noción, las personas tienen derecho a gozar de un ámbito de proyección de su existencia que quede reservado de la invasión y la mirada de los demás, que les concierna sólo a ellos y les provea de condiciones adecuadas para el despliegue de su individualidad -para el desarrollo de su autonomía y su libertad-. A un nivel más concreto, la misma idea puede describirse apelando al derecho de

- La Primera Sala de ese H. Máximo Tribunal ha destacado que el concepto de vida privada comprende además, a la intimidad como el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona, esto es, la vida privada es lo genéricamente reservado y la intimidad -como parte de aquélla- lo radicalmente vedado, lo más personal; de ahí que si bien son derechos distintos, al formar parte uno del otro, cuando se afecta la intimidad, se agravia a la vida privada.[3]
- La SCJN al resolver el Amparo en Revisión 134/2008, determinó que el fundamento del derecho a la privacidad en México es el primer párrafo del artículo 16 constitucional. La privacidad no se acota al espacio físico del domicilio, -lugar donde normalmente se manifiesta la intimidad-, sino que se incluyó también aquellas intromisiones o molestias que por cualquier medio puedan realizarse en el ámbito de la vida privada.
- La Corte Interamericana de Derechos Humanos[4] (CIDH), ha reconocido que el derecho a la privacidad tiene como objeto:
  - Proteger la vida privada y domicilio de injerencias arbitrarias o abusivas; es decir, el derecho de quedar exento de las invasiones por parte de particulares o de las autoridades estatales.
  - Controlar la información de carácter personal, incluso después de haberla proporcionado a un particular o entidad del Estado.
- La CIDH reconoce como elementos inherentes al derecho a la privacidad, el derecho a la vida privada, la inviolabilidad del domicilio, de las conversaciones telefónicas y de cualquier comunicación, el derecho a la honra y la reputación:
  - *Caso de las Masacres de Ituango vs. Colombia*: el domicilio y la vida privada se encuentran intrínsecamente ligados ya que el domicilio se convierte en un espacio en el cual se puede

---

las personas a mantener fuera del conocimiento de los demás (o, a veces, dentro del círculo de sus personas más próximas) ciertas manifestaciones o dimensiones de su existencia (conducta, datos, información, objetos) y al correspondiente derecho a que los demás no las invadan sin su consentimiento. En un sentido amplio, entonces, la protección constitucional de la vida privada implica poder conducir parte de la vida de uno protegido de la mirada y las injerencias de los demás, y guarda conexiones de variado tipo con pretensiones más concretas que los textos constitucionales actuales reconocen a veces como derechos conexos: el derecho de poder tomar libremente ciertas decisiones atinentes al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el espionaje, la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular.
Registro digital: 165823

[3] VIDA PRIVADA E INTIMIDAD. SI BIEN SON DERECHOS DISTINTOS, ÉSTA FORMA PARTE DE AQUÉLLA. La vida se constituye por el ámbito privado reservado para cada persona y del que quedan excluidos los demás, mientras que la intimidad se integra con los extremos más personales de la vida y del entorno familiar, cuyo conocimiento se reserva para los integrantes de la unidad familiar. Así, el concepto de vida privada comprende a la intimidad como el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona, esto es, la vida privada es lo genéricamente reservado y la intimidad -como parte de aquélla- lo radicalmente vedado, lo más personal; de ahí que si bien son derechos distintos, al formar parte uno del otro, cuando se afecta la intimidad, se agravia a la vida privada.
Registro digital: 171883

[4] La reforma constitucional de 2011, en materia de derechos humanos en México, obliga que las autoridades en cualquier ámbito, respeten los instrumentos jurídicos internacionales y la jurisprudencia de tribunales especializados en la protección de derechos humanos, como la Corte Interamericana de Derechos Humanos.

desarrollar libremente la vida privada, por lo que el domicilio se encuentra dentro del ámbito de protección del derecho a la privacidad.[5]

- En el *caso Fontevecchia y D´Amico vs. Argentina*, aunado al reconocimiento del domicilio como elemento de la vida privada, determina que el ámbito de la privacidad comprende entre otras dimensiones, tomar decisiones libremente relacionadas con diversas áreas de la propia vida, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público. En este caso, la CIDH reconoce expresamente el derecho de controlar la información de carácter personal, lo cual se traduce en el derecho a la protección de datos personales.[6]
- *Caso Fernández Ortega y otros vs. México*[7] *y Rosenda Cantú y otra vs. México*[8]: La CIDH incorpora la vida sexual dentro del concepto de vida privada, al señalar que se trata de un término amplio no susceptible de definiciones exhaustivas, pero que comprende, entre otros ámbitos protegidos, la vida sexual y el derecho de establecer y desarrollar relaciones con otros seres humanos. En estos casos, la CIDH establece que ante la violación sexual que sufrieron las víctimas, se vulneraron valores y aspectos esenciales de su vida privada, y supuso una intromisión en su vida sexual, y anuló su derecho a tomar libremente decisiones respecto de con quien tener relaciones sexuales, perdiendo de forma completa el control sobre sus decisiones más personales e íntimas y sobre las funciones corporales básicas.
- *Caso Tristán Donoso vs. Panamá*, la CIDH reconoció que aunque las **conversaciones telefónicas no se encuentren expresamente previstas en el artículo 11 de la Convención Americana sobre Derechos Humanos, se trata de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección de la vida privada**.[9] En este mismo caso, la

[5] Sentencia de 1 de julio de 2006. Caso de las masacres de Ituango vs. Colombia, numeral 7 del apartado de Declaraciones, p. 146. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_148_esp.pdf. Fecha de consulta 20 de agosto de 2018.
[6] Caso Fontevecchia y D´Amico vs. Argentina. Fondo, reparaciones y costas. Sentencia 29 de noviembre de 2011. numeral 48. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf. Fecha de consulta 13 de agosto de 2018.
[7] Caso Fernández Ortega y Otros vs. México. Sentencia de 30 de agosto de 2010. Disponible en: http://www.ordenjuridico.gob.mx/JurInt/STCIDHM2.pdf. Fecha de consulta 13 de agosto de 2018.
[8] Caso Rosendo Cantú y Otra vs. México. Sentencia de 31 de agosto de 2010. Disponible en: http://www.ordenjuridico.gob.mx/JurInt/STCIDHM5.pdf. Fecha de consulta 13 de agosto de 2018.
[9] Caso Tristán Donoso vs. Panamá, numeral 55. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf. Fecha de consulta 20 de agosto de 2018.

CIDH reconoce dos elementos primordiales relacionados al derecho a la privacidad: **la honra y la reputación**, al señalar que el primero se relaciona con la estima y valía propia, mientras que la reputación se refiere a la opinión que otros tienen de una persona.[10]

- El derecho a la privacidad es un concepto extenso dentro de cual se incluyen otros derechos. Como ejemplo de ello, está el derecho a la intimidad, donde si el primero es el ámbito reservado para cada persona y del que quedan excluidos los demás, el segundo se integra con los extremos más personales de la vida y el entorno familiar. Con base en ello, se puede sostener que.
  - La CPEUM y los tratados internacionales reconocen el derecho de toda persona a la vida privada;
  - El derecho a la vida privada origina la posibilidad de las personas a mantener fuera del conocimiento de los demás (incluidas las autoridades) ciertas manifestaciones o dimensiones de su existencia (conducta, datos, información, objetos) y la correspondiente obligación de que los demás no las invadan sin su consentimiento;
  - La intimidad es una vertiente del derecho a la privacidad;
  - El derecho a la intimidad consiste en el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona.
  - Asimismo, el derecho a la intimidad significa el poder de decisión sobre la publicidad o información de datos relativos a su persona.
- La vida privada comprende a la intimidad como el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona, en consecuencia, se puede afirmar que la vida privada es lo genéricamente reservado y la intimidad es lo radicalmente vedado, como es el caso de los datos biométricos que se pretenden recabar y tratar a través del PANAUT, por lo que, en contraposición con lo dispuesto en la CPEUM y los instrumentos internacionales en materia de derechos humanos suscritos por el Estado Mexicano, se advierte que**, la obtención de datos a partir de lo dispuesto en el Decreto, constituye una intervención arbitraria en el ámbito más privado e íntimo de las personas, sin tomar en consideración que todas las personas gozan de un espacio de proyección de su existencia que quede reservado de la invasión y la mirada de los demás, incluso del Estado**, pues en

[10] *Idem*.

esta área es que se desarrolla plenamente la personalidad, vulnera los derechos de privacidad y vida privada, protección de datos personales e intimidad.

- La recopilación y el uso de datos personales por las autoridades de investigación y de procuración de justicia en términos de lo previsto en el Decreto, constituye una injerencia en el derecho a la intimidad, la privacidad y vida privada, y derechos conexos, según lo dispuesto en la CPEUM, el Convenio 108, la LGPDPSO y la LFPDPPP, entre otros instrumentos normativos, y, como tal, **debe basarse en derecho (claro, previsible y accesible)**, **perseguir un objetivo legítimo y limitarse a lo necesario y proporcionado para lograr ese objetivo legítimo.**
- Para que dicha injerencia fuera lícita, todo el tratamiento de datos debería cumplir con los principios **de necesidad, proporcionalidad y limitación de la finalidad.** Esto implica que el tratamiento de datos personales por las autoridades de investigación y de procuración de justicia debe **basarse en fines predefinidos, claros y legítimos establecidos en la ley; debe ser necesario y proporcionado a estos fines legítimos y no debe tratarse de forma incompatible con dichos fines. El tratamiento de datos debe llevarse a cabo de manera legal, justa y transparente. Además, los datos personales tratados por** las autoridades de investigación y de procuración de justicia **deben ser adecuados, pertinentes y no excesivos en relación con los fines. Por último, deben ser precisos y estar actualizados para garantizar la mayor calidad de datos posible.**

- **En relación con el derecho a la protección de datos personales**. Respecto del derecho a la protección de datos personales este Colegio considera absolutamente relevante señalar, en primer lugar que, este derecho "*es un derecho humano reconocido en el artículo 16 de la Constitución Federal- que protege a la persona física identificada o identificable frente al tratamiento ilícito de sus datos personales, otorgándole la facultad de decidir y controlar de manera libre e informada las condiciones y características del tratamiento de sus datos personales, permitiéndole además el ejercicio de determinados derechos y medios de tutela jurídicos para garantía y eficacia práctica de estos últimos*". La emisión del Decreto y la creación del PANAUT vulnerar este derecho por las siguientes razones:
  - La normatividad de desarrollo de los sectores público y privado (La Ley Federal de Protección de Datos Personales en Posesión de los

Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la normatividad de desarrollo de las mismas) configura un conjunto de principios y deberes para el que trata los datos Principios (***licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad*** **y** ***responsabilidad)***; y Deberes: (***seguridad*** y ***confidencialidad***), unos derechos para los titulares (acceder a sus datos, solicitar su rectificación en caso de que sean inadecuados o excesivos, pedir su cancelación, y manifestar su oposición al tratamiento, esto es, el famoso acrónimo ARCO, añadiéndose en la normatividad del sector público el derecho a la portabilidad), y unas garantías de protección en caso de que esos derechos se vean infringidos o el tratamiento de los datos personales haya incurrido en algún otro tipo de violación.

- Estos principios, deberes y derechos configuran al derecho humano a la protección de datos personales como tal, de modo que constituyen su núcleo básico o esencial **y por tanto cualquier fallo o violación de cualquiera de estos principios que configuran este derecho humano implica una violación del propio derecho**.
- El Decreto resulta inconstitucional toda vez que la creación del PANAUT implica una indubitable transgresión de los principios y deberes de protección de datos previstos en la LFPDPPP y la LGPDPPSO como se expone a continuación:
  - ***Violación al principio de licitud:*** La violación al principio de licitud que configura el derecho a la protección de datos se materializa con la creación del Padrón porque el IFT carece de facultades y atribuciones para instalar, operar, regular y mantener el PANAUT de acuerdo con la finalidad del mismo. Derivado de la propia naturaleza del Padrón ya se advierte la ausencia de habilitación legal al IFT para gestionar dicho registro, pues:
    - El IFT como órgano regulador de los sectores de telecomunicaciones y radiodifusión, no cuenta con ninguna atribución y/o facultad legal que le legitime para el ejercicio de ninguna de las dos funciones señaladas, y
    - La gestión del derecho a la identidad está reservada a la Secretaría de Gobernación, a través del Registro Nacional de Población,[11] como reserva de ley expresa, formal y material, mediante la Ley General de Población cuyo artículo 85 establece que la SEGOB

[11] Artículo 86.- El Registro Nacional de Población tiene como finalidad registrar a cada una de las personas que integran la población del país, con los datos que permitan certificar y acreditar fehacientemente su identidad.

tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero,[12].

- En definitiva, existe, una ilegitimidad para el IFT de doble vertiente: activa (invasión de la esfera de atribuciones y facultades de la SEGOB) y pasiva (carencia de atribuciones).
- En virtud de lo anterior, se puede considerar que el hecho de que el legislador federal atribuya al IFT una facultad legal, **contraria a lo establecido por el texto constitucional resulta violatoria de los derechos humanos de legalidad y seguridad jurídica, al constituir una ampliación arbitraria e infundada de las atribuciones constitucionales de dicho órgano regulador con base en lo dispuesto por el artículo 28 de la CPEUM, que además supone una intromisión ilícita en las facultades y competencias de otras autoridades que están legalmente facultadas para las materias que se pretenden atribuir ilícitamente al IFT.**

- ***Violación al principio de finalidad***. El Decreto y la creación del PANAUT violan el principio de finalidad por las siguientes razones:
  - El principio de finalidad regulado tanto en el Convenio 108 como en la LFPDPPP y en la LGPDPPSO establece la obligación de que la obtención y tratamiento de los datos personales deberán sujetarse a finalidades **explícitas, legítimas y determinadas.**
  - En relación con el referido principio, el Convenio 108, en su artículo 5, obliga al Estado Mexicano a establecer medidas para que los datos personales en posesión de sujetos obligados, como lo es el IFT, únicamente sean sujetos a tratamiento cuando **existan fines determinados y legítimos**, prohibiéndose su utilización de forma incompatible con dichos fines. En el presente caso es indudable que el Decreto reclamado vulnera el principio de finalidad y por ende el derecho humano de protección de datos personales en virtud de que:

[12] Artículo 85.- La Secretaría de Gobernación tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero.

- La finalidad explícita por la que se pretende justificar el **Padrón** (colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos cometidos a través de líneas celulares) no resulta adecuada o racional porque no constituye una medida que permita alcanzar el fin perseguido, y es en realidad una finalidad eventual respecto de la **verdadera finalidad** que consiste en la "identificación plena y certera de los titulares de las líneas de comunicación, a través del Padrón" y, solo de forma eventual, en caso de cometerse un delito con la línea celular, emplear esa información para su persecución, por lo que el Padrón tiene un fin primario de registro y control de las personas a través de líneas telefónicas móviles, desde el momento de su adquisición, y
- El IFT carece de atribuciones o competencias para la realización de este tratamiento, e invade competencias reservadas formal y materialmente por ley.

- ***Violación al principio de proporcionalidad***. Se configura una violación al principio de proporcionalidad previsto en la normatividad vigente en virtud de lo siguiente:
  - El principio de proporcionalidad está previsto en el artículo 5o, inciso c, del Convenio 108, el cual determina que los datos de carácter personal que los Estados recopilen serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado, situación que no se cumple con la sola creación del PANAUT que ordena recabar datos biométricos sensibles sin que exista una adecuada justificación legal.
  - La LGPDPPSO – artículo 25 - y la LFPDPPP – artículo 13-, de forma similar, establecen que **el responsable solo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento,** situación que no se cumple con la sola creación del PANAUT que ordena recabar datos

biométricos sensibles sin que exista una adecuada justificación legal.

- El Decreto **vulnera el principio de proporcionalidad** y por ende el derecho humano de protección de datos personales en virtud de que, como se demostrará a continuación:
    - Los datos personales objeto del tratamiento del Padrón **son excesivos** para la finalidad de colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos cometidos a través de líneas celulares, ya que los datos personales objeto del tratamiento del Padrón son de una naturaleza tendiente a crear un registro de identidad que permiten certificar y acreditar fehacientemente la identidad de los ciudadanos, finalidad que no es compatible con la finalidad para la cual fue creado el Padrón.
    - Obliga al tratamiento de **datos personales biométricos**, mismos que constituyen datos personales sensibles sin que exista legitimación alguna que lo permita ni sea proporcional su tratamiento.
    - Existe una **conservación injustificada** de los datos personales de los usuarios sin limitación de los periodos de retención. En particular, para el tratamiento de datos personales sensibles, el responsable del tratamiento está obligado a realizar esfuerzos razonables para limitar el periodo de tratamiento al mínimo indispensable.
    - En particular, **no se permite la supresión** de los datos cuando los usuarios dan de baja su línea celular, sino que, sin justificación alguna, se mantendrán durante 6 meses.

- ***Violación al principio de responsabilidad***.
    - La normatividad aplicable en materia de protección de datos personales exige, **en cumplimiento del principio de responsabilidad, previsto en los artículos 14 de la LFPDPPP y 74 de la LGPDPPSO,** que el responsable del tratamiento realice una **Evaluación de Impacto en la Protección de Datos**

Personales (en adelante "EIPDP") cuando exista la probabilidad de que, por su naturaleza, alcance o fines, las operaciones de tratamiento entrañen un alto riesgo para los derechos y las libertades de los titulares de datos personales. Es decir, cuando exista un tratamiento intensivo o relevante de datos personales. En este contexto, se debe recordar que la EIPD:

- Tiene que realizarse de manera previa al tratamiento que se "pretenda poner en operación" que suponga un tratamiento intensivo. Así expresamente el articulo 77 de la LGPDPPSO y el artículo 23 de las Disposiciones EIPDP indican que, los sujetos obligados que realicen una EIPDP, deberán presentarla ante el INAI (o los organismos garantes) cuando menos **treinta días antes** a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, a efecto de que se emita el dictamen correspondiente en los treinta días siguientes (ex art. 78 LGPDPPSO).
- Uno de sus objetivos principales es identificar y describir los altos riesgos potenciales y probables que entrañen los tratamientos intensivos o relevantes de datos personales.
- Se basa en el contraste entre la situación de partida y lo que ocurre una vez que el tratamiento tenga lugar. Ese contraste busca revelar los cambios que se pueden atribuir al tratamiento realizado.
- Derivado de las conclusiones en esa evaluación habrá que decidir si ese tratamiento se puede llevar a cabo, y, en su caso, con qué medidas de seguridad.
- Tal y como el mismo Dictamen de reforma a la LFTR del 16 de abril de 2021 reconoce: *(…)* ***v. Será necesario realizar una evaluación de impacto a la protección de datos personales****,*

mismo que implica la vulneración de los datos que son confidenciales"

- El simple hecho de que el Legislador haya sido omiso en realizar una apreciación de proporcionalidad (*test de proporcionalidad*) respecto de la creación del PANAUT en relación con la restricción al derecho humano a la protección de datos personales e instruir al IFT como órgano responsable del tratamiento de datos relativos al PANAUT llevar a cabo una EIPDP, **es violatorio del derecho humano de protección de datos personales por incumplimiento al principio de responsabilidad.**

- ***Violación al deber de seguridad***. En relación con la violación al deber de seguridad es importante tomar en cuenta lo siguiente:
  - Tanto en la LFPDPPP como en la LGPDPPSO la obligación de seguridad se regula como un deber, y por lo tanto, como una obligación proactiva, preventiva y demostrable para todos los responsables del tratamiento sean estos entes públicos o privados, obligándoles dicho deber a establecer y mantener diversos controles de seguridad administrativos, físicos y técnicos para evitar que la confidencialidad, integridad y disponibilidad de la información se vean comprometidas.
  - No puede obviarse que los costos de implementar medidas de seguridad como las que se requiere para garantizar la seguridad de los datos personales que son objeto del tratamiento en el PANAUT son significativos, aunado a los recursos humanos requeridos para su implementación. Ahora bien, en el presente caso existe evidencia objetiva **en cuanto a que el cumplimiento de este deber de seguridad resulta de imposible cumplimiento tanto para el IFT como para los concesionarios** como se evidencia en los siguientes textos:
    - Entrevista del CP Adolfo Cuevas a Multimedios. Tema: Padrón Nacional de Usuarios de Telefonía Móvil..[13]

[13] http://www.ift.org.mx/secciones/entrevistas

- IFT aclara que para el padrón son 800 mdp que no tiene.[14]
- IFT, SIN RECURSOS PARA ARRANQUE DEL PADRÓN TELEFÓNICO.[15]
- El IFT requerirá más presupuesto para el padrón de celulares..[16]
- El Padrón de Usuarios de Telefonía Móvil requerirá una inversión de más de 700 millones de pesos en México: IFT..[17]

- De lo anterior se advierte que el IFT ha reconocido públicamente **que le es imposible destinar recurso alguno a la instalación, operación, regulación y mantenimiento del PANAUT, lo que significa que una de las bases de datos más sensibles e importantes del país, en cuanto a que un mal uso de los datos personales ahí contenidos tendría como consecuencia afectaciones irreparables para los titulares de los datos personales, no contendrá control de seguridad alguno, ya que no existe presupuesto para ello.**
- En relación con lo anterior no puede pasar desapercibido que los datos personales contenidos en el PANAUT tendrán un valor en el mercado extremadamente alto, por lo que dicha base de datos será susceptible de múltiples ataques en materia de ciberseguridad, en especial si tenemos como referencia los siguientes sucesos que se han presentado, en los últimos años, con bases de datos en posesión de entidades gubernamentales como se desprende de las notas siguientes:
  - RENAUT: [18]
  - 2020, en 12 hackeos o incidentes de seguridad en México..[19]
  - Anonymous hackea el portal de Condusef y amaga con
  - derribar el sitio web de Banxico.[20].

[14] https://www.razon.com.mx/negocios/ift-recursos-arranque-padron-telefonico-431459
[15] *https://cirt.mx/ift-sin-recursos-para-arranque-del-padron-telefonico/?utm_source=rss&utm_medium=rss&utm_campaign=ift-sin-recursos-para-arranque-del-padron-telefonico*
[16] https://www.informador.mx/economia/El-IFT-requerira-mas-presupuesto-para-el-padron-de-celulares-20210426-0004.html
[17] https://www.xataka.com.mx/telecomunicaciones/padron-usuarios-telefonia-movil-requerira-inversion-700-millones-pesos-mexico-ift
[18] https://www.animalpolitico.com/2012/06/segob-elimina-base-de-datos-del-renaut/
[19] https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html

- CONDUSEF alerta a los usuarios de Servicios Financieros de un virus que podría secuestrar la información de tu equipo de cómputo..[21]
- Atacantes ofertan base de datos de Condusef tras ataque al sitio. .[22]
- Ayer fue la Condusef; hoy Banxico sufre ataque en su sitio web.[23]
- Ataque de hackers a Banxico: [24]
- Información sobre los Ataques a Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI).[25]
- Reporta SAT ataque cibernético.[26].
- El SAT informa que sus sistemas sufrieron ataque externo, pero ya funcionan con normalidad..[27]
- STPS reporta "incidente" en sus servicios de cómputo..[28]
- Secretaría de Trabajo reporta "incidente" que afectó infraestructura de cómputo..[29]
- Secretaría de Economía suspende trámites por ataque cibernético..[30]
- Controla Secretaría de Economía ataque informático.[31]
- Desactivan página de Conapred tras cuatro ataques cibernéticos.[32].
- Los empleados de Pemex denuncian "secuestro informático".[33]
- Los hackers reclamaron 4.9 mdd a Pemex para liberar su información.[34].
- Función Pública expuso la declaración patrimonial de 830,000 funcionarios públicos.[35].

---

[20] https://www.eleconomista.com.mx/politica/Anonymous-hackea-el-portal-de-Condusef-y-amaga-con-derribar-el-sitio-web-de-Banxico-durante-la-mananera-de-AMLO-20200706-0088.html
[21] https://www.condusef.gob.mx/?p=contenido&idc=498&idcat=1
[22] https://elceo.com/tecnologia/atacantes-ofertan-base-de-datos-de-condusef-tras-ataque-al-sitio/
[23] https://expansion.mx/economia/2020/07/07/banxico-sufre-ataque-en-su-sitio-web
[24] https://silent4business.com/ataque-de-hackers-a-banxico-que-sucedio/
[25] https://www.banxico.org.mx/publicaciones-y-prensa/informes-trimestrales/recuadros/%7B86A498AE-5F8A-57CE-2C11-B5059AB9EB20%7D.pdf
[26] https://www.elmananerodiario.com/reporta-sat-ataque-cibernetico/
[27] https://www.sinembargo.mx/09-07-2020/3820236
[28] https://www.razon.com.mx/mexico/ciberataque-stps-reporta-incidencia-en-sus-servicios-de-computo/
[29] https://www.milenio.com/politica/stps-fallan-servidores-de-computo-de-la-secretaria-del-trabajo
[30] https://www.eleconomista.com.mx/tecnologia/Secretaria-de-Economia-suspende-tramites-por-ataque-cibernetico-20200224-0085.html
[31] https://www.gob.mx/se/articulos/controla-secretaria-de-economia-ataque-informatico?idiom=es
[32] https://www.excelsior.com.mx/nacional/desactivan-pagina-de-conapred-tras-cuatro-ataques-ciberneticos/1389902
[33] https://expansion.mx/tecnologia/2019/11/12/los-hackers-han-reclamado-4-9-mdd-pemex-liberar-informacion
[34] https://expansion.mx/tecnologia/2019/11/12/los-hackers-han-reclamado-4-9-mdd-pemex-liberar-informacion
[35] https://www.eleconomista.com.mx/politica/Funcion-Publica-expuso-la-declaracion-patrimonial-de-830000-funcionarios-publicos-20200704-0009.html

- Función Pública incumplió con la ley por fuga de datos personales:..[36]
- Vulneración de datos personales en el ISSSTE..[37]
- Extorsión a la Comisión Nacional de Seguros y Fianzas.[38].
- Esto es todo lo que sabemos del hackeo a la Comisión Nacional de Seguros y Fianzas..[39]

- En virtud de los principios de interdependencia de los derechos humanos, los impactos adversos relacionados con la incorporación de novedosos tratamientos que emplean ingentes cantidades de datos, pueden comprometer un amplio espectro de derechos, entre otros, **el derecho a la igualdad de protección de la ley sin discriminación, los derechos a la vida, a la libertad y seguridad de la persona, un juicio justo y debido proceso, el derecho a la libertad de movimiento, el derecho a disfrutar del más alto nivel posible de salud, y tener acceso al trabajo y la seguridad social. Estas preocupaciones se agravan aún más en cuando se realizan tratamientos de datos biométricos de manera intensiva y a gran escala**.
- La creación del Padrón, supuestamente con el fin eventual de la colaboración con las autoridades de investigación y de procuración de justicia, **supone la dejación de la función de investigación del Estado en manos de particulares, creando una suerte de "justicia automática", donde la lista -sin importar que además puede contener multitud de sesgos- contiene a los sospechosos de manera inmediata, vulnerando no solo el principio de presunción de inocencia, sino el de debido proceso**.
- El impacto en los derechos humanos vinculado al uso de herramientas y datos biométricos es enorme. Las consecuencias relacionadas se sienten en una variedad de derechos fundamentales, incluidos, entre otros, los derechos a la vida**, la dignidad humana, la libertad, la libertad de expresión y la seguridad de la persona, el derecho a no ser sometido a tortura, tratos crueles, inhumanos o degradantes, el derecho al acceso a la justicia, la privacidad y la vida familiar, la libertad de expresión o movimiento, etc. La escala de la afectación, junto**

[36] https://www.eleconomista.com.mx/politica/Funcion-Publica-incumplio-con-la-ley-por-fuga-de-datos-personales-Inai-20201124-0082.html
[37] https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html
[38] https://www.eleconomista.com.mx/tecnologia/2020-en-12-hackeos-o-incidentes-de-seguridad-en-Mexico-20210102-0007.html
[39] https://www.eleconomista.com.mx/sectorfinanciero/Esto-es-todo-lo-que-sabemos-del-hackeo-a-la-Comision-Nacional-de-Seguros-y-Fianzas-20201208-0048.html

con la naturaleza universal, interdependiente e interconectada de estos derechos, conlleva efectos múltiples e interrelacionados en una serie de situaciones individuales y colectivas.

- **En relación con el derecho a la identidad**. Coincidimos con el máximo órgano garante de la protección de datos personales en nuestro país en que, el Decreto vulnera el derecho humano a la identidad de las personas reconocido en el artículo 4 constitucional por las siguientes razones:
    - El derecho a la identidad como todo derecho humano, es universal, no puede tener caducidad, es único, irrenunciable, intransferible e indivisible.
    - Constituye el derecho primigenio que se convierte de manera automática en la llave de acceso a otros derechos esenciales como el derecho a la salud, a la educación, a la protección y a la inclusión en la vida económica, cultural y política del país para cualquier persona.
    - El derecho a la identidad es muy importante para el bienestar no sólo de la persona, sino para beneficio de la sociedad es un derecho elemental que lleva consigo elementos tanto de origen como de identidad personal.[40]
    - El Derecho a la Identidad tiene dos pilares fundamentales para su ejercicio, la identidad jurídica y la identidad biométrica, ligadas a través del identificador único que es la CURP, y así garantizar su unicidad, sin la cual no hay identidad.
    - En un país federal como el nuestro, la tarea de garantizar la identidad la compartimos el gobierno federal y los gobiernos de las 32 entidades federativas, quienes a través de sus Registros Civiles acreditan la identidad jurídica de las personas; es por ello que, respetando la soberanía estatal, se ha trabajado conjuntamente para reforzar este pilar.
    - La identidad se construye a través de múltiples factores psicológicos y sociales de la manera en la que el individuo se concibe y los rasgos definitorios de su personalidad.[41] La identidad no es sólo jurídica, implica una identidad personal, biológica, de género, social y cultural y permite a las personas:

[40] CÁSARES GARCÍA, Leonel. Noción básica del derecho a la identidad en México. Hechos y Derechos, [S.l.], may 2015. ISSN 2448-4725. Disponible en: <https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/7232/9168>. Fecha de acceso: 22 may 2021

[41] Tesis: 1a. XLIV/2012 (10a.), Primera Sala, Semanario Judicial de la Federación y su Gaceta. Libro VI, Marzo de 2012, Tomo 1, página 274

- Saber quiénes son y distinguirse de los demás.
- Tener una nacionalidad que los vincula con un Estado determinado y gozar de todos los derechos que éste les reconoce.
- Accesar a servicios y prestaciones que contribuyen a la satisfacción de otros derechos como a la salud, a la educación, a programas sociales, entre otros.

- El derecho a la identidad tiene un gran valor instrumental al ser necesario para el ejercicio de otros derechos civiles, políticos, económicos y culturales, así como obligaciones. En este sentido, en la tesis 1a. LXXV/2018 (10a.) localizable en la Gaceta del Semanario Judicial de la Federación, Libro 55, Junio de 2018, Tomo II, página 956 se precisa que este derecho "constituye un derecho que puede comprender otros derechos, como el derecho al nombre, a la nacionalidad y a conocer su filiación y origen y a partir de esos derechos se pueden derivar otros distintos, como son los de alimentación, educación, salud y sano esparcimiento."
- *La identidad es la característica de ser una persona en concreto y no otra, lo cual se determina por un conjunto de atributos que la diferencian y la vuelven única*. El conjunto de atributos puede integrarse por la suma de rasgos y datos personales inherentes al individuo (altura, edad, fecha de nacimiento, biometrías, etc.), así como rasgos acumulados en el tiempo (expedientes médicos, preferencias, comportamientos, etc.) y datos asignados por entes públicos y/o privados (teléfono, email, No. empleado, RFC, CURP o No. del pasaporte).
- **Los datos biométricos son uno de los elementos que configuran el derecho a la identidad,** pues como hemos dicho, tienen el carácter de únicos, inherentes y en muchos casos permanentes a lo largo de la vida de sus titulares, por lo que, sin duda alguna la función identificadora es uno de sus atributos más relevantes.
- **La pérdida de estos datos, en muchos casos es irremplazable.** No es posible, por la misma naturaleza de los mismos, cambiar las huellas digitales, o la voz, o el reconocimiento facial, el iris… Se podrá pedir alternativamente uno u otro, pero el individuo no podrá cambiarlos, y la afectación al mismo será muy relevante, no solo en el entorno en que sucedió, sino en muchas otras esferas de su vida, y para siempre.
- En México, particularmente, las cifras del denominado delito de "robo o usurpación de identidad" son muy altas. Por ejemplo, en los primeros tres meses de 2021 se registraron más de 21,500

denuncias por fraude y casi 2,000 por extorsión en el país. En el caso del fraude, las denuncias van al alza desde 2018. En México se han registrado 786 denuncias por falsedad–así clasifica el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) el robo de identidad– en los primeros tres meses de 2021.[42] Las consecuencias también son muy graves, pero, si además esa usurpación se da sobre datos biométricos, las repercusiones, no solo para los afectados, sino para el entorno y/o mercado donde se produjo, además de las posibles afectaciones consecuentes en otros entornos, pueden ser devastadoras e irreversibles, insistimos, no solo por la afectación real, sino por la imposibilidad de la remediación.

- Todo aquél que trate datos personales, ya sea en su calidad de responsable o encargado del tratamiento, por lo tanto, está sujeto a unas medidas de seguridad físicas, técnicas o administrativas reforzadas, relacionadas con precisos deberes de cuidado establecidos en leyes, habiendo realizado previamente el correspondiente análisis de riesgos, que además tendrá que ser actualizado e igualmente las medidas en correlación al mismo.
- El Decreto ya avanza que va a contener los datos biométricos -dejando su especificación, vulnerando el principio de legalidad, al IFT- de los usuarios. Además, en la recolección y tratamiento de los mismos habrá diversos -en número, capacidades y circunstancias- intervinientes. Los concesionarios y autorizados serán los que los recopilarán, se transmitirán al IFT, y éste los tendrá a disposición de multitud de autoridades de investigación y procuración de justicia.
- **El Decreto no establece ninguna medida de seguridad**. Es decir, la ley que regula la creación del Padrón no establece ningún deber de cuidado en un tratamiento intensivo, a gran escala de datos especialmente sensibles, alimentados y manejados por multitud de intervinientes, y cuya pérdida generaría una afectación irremediable a sus titulares y al entorno, en este caso a todo el país y a todos los mercados en los que se utilizaran esos datos, es decir, a toda la sociedad en su conjunto, de manera irreversible. No existen mecanismos de protección y/o asignación de responsabillidades previstos por el Decreto. Por el contrario, en el único momento que se menciona alguna medida tecnológica, en el artículo 180 Quintes, es para incentivar y hacer más fácil la recopilación masiva de datos y la integración del padrón al señalar la posibilidad de recabar los

[42] El índice de robo de identidad en México regresó a niveles pre pandemia, CUESTIONE, abril, 2021, disponible en *https://cuestione.com/nacional/robo-identidad-mexico-tarjetas-credito-fraude-datos-usuarios/*

datos biométricos y el domicilio del usuario, a través de medios digitales o medios remotos.

- La gestión del derecho a la identidad está reservado a la Secretaría de Gobernación, a través del Registro Nacional de Población,[43]como reserva de ley expresa, formal y material, mediante la Ley General de Población (en adelante "LFP") cuyo artículo 85 establece que la SEGOB tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero.
- Con la creación del PANAUT bajo el IFT, se consiguen dos objetivos de gran relevancia para la Administración de manera ilícita: por un lado, la SEGOB conseguiría una base de datos de mayor alcance -en número de individuos y tipo de datos-, de manera gratuita y, por otro, el PANAUT nace con la vocación de estar a disposición de las autoridades de investigación y procuración de justicia. Por eso, el PANAUT es ilegítimo e ilícito: porque la gestión de la identidad está reservada por ley a otra autoridad, y porque el acceso por dichas autoridades no puede carecer de garantías.
- Atribuir la gestión del derecho a la identidad al IFT supone también una intromisión a una facultad explícita y reservada formal y materialmente por ley**.** La Ley General de Población -como ley formal y materialmente válida- **otorga a la Secretaría de Gobernación las facultades en materia de registro de población e identidad** que se indican en el artículo 85 de la Ley General de Población. Además, basta recordar que, de acuerdo con la jurisprudencia de nuestro máximo tribunal el hecho de que el IFT sea un órgano constitucionalmente autónomo no implica que este último no deba subordinarse al principio de reserva de Ley.
- El PANAUT genera **una grave afectación al derecho de identidad, de imposible reparación**, porque **la no exigencia legal de medidas de cuidado y seguridad (administrativas, físicas y técnicas) para acceder, alimentar y en general tratar los datos biométricos que serán incluidos y accedidos a través del PANAUT por la amplitud de sujetos involucrados en el tratamiento de esos datos deriva en una amenaza real e inminente que vulnera el derecho de identidad de los usuarios de telefonía móvil.**

[43] Artículo 86.- El Registro Nacional de Población tiene como finalidad registrar a cada una de las personas que integran la población del país, con los datos que permitan certificar y acreditar fehacientemente su identidad.

- **<u>En relación con el interés superior de la niñez mexicana</u>**. Este Colegio coincide con el INAI en que el Decreto vulnera los derechos de los niños, niñas y adolescentes mexicanos y en interés superior de la niñez por las razones siguientes:
    - De acuerdo con la Jurisprudencia 2a./J. 113/2019 (10a.) de la Segunda Sala de nuestro Máximo Tribunal el derecho del interés superior del menor prescribe que se observe "en todas las decisiones y medidas relacionadas con el niño", lo que significa que, en "cualquier medida que tenga que ver con uno o varios niños, su interés superior deberá ser una consideración primordial a que se atenderá", lo cual incluye no sólo las decisiones, sino también todos los actos, conductas, propuestas, servicios, procedimientos y demás iniciativas."
    - En relación con el principio de interés superior del niño, la CIDH señala que:
        - Este principio regulador regulador de la normativa de los derechos del niño se funda en la dignidad misma del ser humano, en las características propias de los niños, y en la necesidad de propiciar el desarrollo de éstos, con pleno aprovechamiento de sus potencialidades así como en la naturaleza y alcances de la Convención sobre los Derechos del Niño[44].
        - La expresión "interés superior del niño", consagrada en el artículo 3 de la Convención sobre los Derechos del Niño, implica que el desarrollo de éste y el ejercicio pleno de sus derechos deben ser considerados como criterios rectores para la elaboración de normas y la aplicación de éstas en todos los órdenes relativos a la vida del niño.[45]
        - La verdadera y plena protección de los niños significa que éstos puedan disfrutar ampliamente de todos sus derechos, entre ellos los económicos, sociales y culturales, que les asignan diversos instrumentos internacionales. Los Estados Partes en los tratados internacionales de derechos humanos tienen la obligación de adoptar medidas positivas para asegurar la protección de todos los derechos del niño.[46]
    - Al estar reconocido el derecho a la identidad en los artículos 7o. y 8o. de la Convención sobre los Derechos del Niño (CADN), es innegable su rango constitucional. Asimismo, de acuerdo a dichos preceptos y

[44] 22 Corte Interamericana de Derechos Humanos, Condición jurídica y derechos humanos del niño. Disponible en: https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica_opinion.cfm?nId_Ficha=17&lang=es
[45] Corte IDH. Condición jurídica y derechos humanos del niño. Opinión Consultiva OC-17/02 de 28 de agosto de 2002. Serie A No. 17.
[46] Corte IDH. Condición jurídica y derechos humanos del niño. Opinión Consultiva OC-17/02 de 28 de agosto de 2002. Serie A No. 17.

al artículo 22 de la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes (en adelante "LPDNNA"), el derecho a la identidad está compuesto por el derecho a tener un nombre, una nacionalidad y una filiación. [47]

- El Decreto no distingue entre los diferentes grupos de usuarios a los que se les tomarán los datos y ordena una obtención indiscriminada y desproporcionada de datos personales de todos tipos de personas, incluyendo población vulnerable conformada por niñas, niños y adolescentes. En este sentido, dado el gran número de niños que poseen un celular, es deducible que, por la obligación expuesta del decreto, se recabarán los datos de muchos de ellos.
- De acuerdo con CPEUM, tratados internacionales, leyes vigentes y Jurisprudencia de nuestro máximo tribunal, *"cualquier medida o acto que tenga un impacto en la esfera de los niños, niñas o adolescentes debe atender al principio de interés superior del menor en virtud de que se trata de un grupo en situación de vulnerabilidad. Cualquier medida limitativa de derechos de los niños siempre debe cumplir con el requisito de ser "en el interés superior del niño*". Esto significa que las consideraciones relacionadas con el interés superior del niño deben informar la evaluación de si la medida limitativa del derecho en cuestión es necesaria y proporcional.
- En particular, en relación con las actividades de investigación y procuración de justicia, el Estado Mexicano tiene la obligación de proteger a los niños, niñas y adolescentes contra todas las formas de discriminación o castigo sobre la base del estado, las actividades, las opiniones expresadas o las creencias de los padres, tutores legales o miembros de la familia del niño, niña o adolescente, lo que resulta de suma importancia al dirigirse a niños asociados con grupos terroristas, incluidos familiares de "combatientes terroristas extranjeros" conocidos o presuntos.
- La recolección de datos biométricos sin periodo de retención o cancelación prevista en el Decreto, en el caso de los niños, niñas y adolescentes puede dar lugar a más sesgos y ser menos estables (ya que pueden sufrir alteraciones como resultado del proceso de crecimiento o envejecimiento). Es decir, si el daño que el PANAUT ya causa a la población en general es de por sí irreparable, en el caso de grupos vulnerables, las consecuencias serán mucho más nocivas, tratándose de un grupo en situación de vulnerabilidad como el caso de niños, niñas y adolescentes.

[47] Tesis 1a. CXVI/2011, emitida por la Primera Sala de la Suprema Corte de Justicia de la Nación, visible en el semanario judicial de la federación y su gaceta, tomo XXXIV, septiembre de 2011, página 1034

- El Decreto viola el derecho humano a la identidad de niños, niñas y adolescentes, así como el principio de interés superior del menor previstos en el párrafo octavo del artículo 4 constitucional, artículo 7, 8 y 16 de la CADN, artículo 6 de la DUDH, artículos 3 y 18 de la CADH, artículos 16 y 24 del PIDCP y párrafo segundo, artículo 2 y artículo 19 de la LPDNNA.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucionales las disposiciones del Decreto por ser contrarias a los artículos 1o, 6o, segundo y tercer párrafos; apartado A, fracciones II, III y VIII, párrafos primero y segundo, 14, 16, 28, 73, fracciones XXIX-O y XXIX-S; y, 133 de la CPEUM; 11 de la CADH; 17 del PIDCP; 12 de la DUDH; 5, 7 y 8 del Convenio 108; 1° de su Protocolo Adicional y, 8 y 16 de la CADN.

2. Segundo concepto de invalidez

Como segundo concepto de invalidez el INAI indica los artículos 15, fracción XLII bis, 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), 180 Sextus, 180 Septimus, Primero, Cuarto y Quinto Transitorios del Decreto, al establecer la creación del PANAUT, que contendrá información y datos personales, son violatorios de los derechos relativos a la vida privada o privacidad de las personas y a la protección de los datos personales, contenidos en los diversos 6o, Apartado A, fracción II, y 16 constitucionales, y 11 de la CADH, 17 del PIDCP, 12 de la DUDH y V de la DADDH, puesto que la medida es desproporcional.

Derivado de esto, en su segundo concepto de invalidez el INAI sostiene que, el sistema normativo el Decreto ordena la recopilación, obtención, registro, conservación, almacenamiento, acceso, utilización, comunicación, posesión, manejo y transferencia de los datos personales, incluidos datos personales sensibles, lo cual implica una intervención y/o restricción al derecho a la protección de los datos personales sin que la misma cumpla con los parámetros para el efecto. En este sentido, el INAI sostiene las siguientes premisas:

- Se observa que la protección de los datos personales que permiten la identificación de las personas abarca las diferentes acciones que la reforma implica: recopilación, obtención, registro, conservación, almacenamiento, acceso, utilización, comunicación, posesión, manejo y transferencia de datos personales y sensibles, por lo que los artículos impugnados inciden en el contenido esencial del derecho en cuestión, de ahí que ahora habrá de determinarse si la medida (recopilación, obtención, registro, etc.) persigue un: ***Fin constitucionalmente válido***.

- El Decreto, precisa de manera textual en su artículo 180 bis, que el único fin del padrón es el de colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos en los términos de las disposiciones jurídicas aplicables. En una primera aproximación, se observa que la finalidad del Padrón es constituirse en una *herramienta instrumental para el combate a determinados ilícitos que utilizan la telefonía móvil como instrumento o medio comisivo.*
- Para la correcta apreciación de la finalidad de la medida legislativa, el análisis debe segmentarse en dos momentos:
    - Por un lado, la finalidad de la reforma a la LFTR en su razón ontológica y esencia de ser. Y, por el otro, la finalidad del PANAUT que, si bien comparte la teleología de la modificación legislativa, es consecuencial. Dicho de otra forma, la finalidad de la modificación legislativa se materializa en la creación del Padrón y, la finalidad de éste, será "colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos". De modo que se tienen dos finalidades que es preciso analizar: la creación del padrón y la colaboración en materia de seguridad y justicia.
- La intencionalidad de cada una de las propuestas de reforma atiende a la creación de un sistema que registre y controle líneas telefónicas móviles desde el momento de su adquisición, que permita aportar datos del usuario y dueño de la línea, supervisión del concesionario y vigilancia por parte de la autoridad competente. Así, es posible concluir que la finalidad de dichas iniciativas de reforma a la LFTR, se materializa en el registro y control de líneas telefónicas, y solo una vez obtenido dicho registro, a la postre el PANAUT, es que, a decir de las propias motivaciones, se contará con información relacionada con la comisión de algún ilícito.
- La intención consiste en contar con un Padrón que integre todos los datos de las personas, datos que, en el dado caso que se cometa un delito, podrán ser empleados para su investigación. De ello se sigue que, en realidad, el fin es la formación de una base de datos con la información privada de todos los mexicanos, para su registro, supervisión y control, y sólo de forma contingente, esto es, si se llegare a cometer un delito, los datos serían usados para las labores de seguridad pública. De lo contrario, de no cometerse ningún ilícito, entonces el único fin es la creación de un Padrón que registre, controle y supervise de todos los ciudadanos, aún a los niños.
- En esa medida es que se considera importante considerar que la colaboración en materia de seguridad y justicia, es contingente a la creación del propio Padrón. Diferente es si el padrón colmará aquellos

objetivos. Es decir, si en efecto, contar con todos los datos personales de los mexicanos se inhibirán los delitos cometidos vía telefonía móvil. Por ende, lo que aquí se advierte, es que desde el inicio del proceso legislativo la finalidad de la medida normativa que entró en vigor el 16 de abril de 2021, no es la colaboración en materia de seguridad y justicia, sino la creación de un registro de usuarios de telefonía móvil y es sobre esto, que debe ser analizada su validez constitucional.

- Tanto de los dictámenes aludidos, como de las exposiciones de motivos transcritas, es posible desprender el hecho de que la finalidad del PANAUT es la inhibición de delitos y la colaboración con las autoridades competentes en materia de seguridad y justicia. Sin embargo, la intencionalidad primaria de la reforma es la "identificación plena y certera de los titulares de las líneas de comunicación, a través del Padrón" y, de forma contingente, en caso de cometerse en delito, emplear esa información para su persecución.
- Se advierte entonces que son dos finalidades las que conviven al mismo tiempo de forma paralela: la inhibición de delitos y "la identificación de los titulares de las líneas telefónicas, a través del sistema que controle y registre datos personales de sus propietarios". De ello, es necesario cuestionar si una modificación legislativa en tanto causa, puede tener dos finalidades diversas, como consecuencia. En el supuesto que nos ocupa, la finalidad primaria de la reforma a la LFTR consiste en crear un sistema que registre y controle líneas telefónicas móviles desde el momento de su adquisición. La inhibición de los delitos y la colaboración con las autoridades en materia de seguridad y justica, es secundaria a la finalidad principal y sólo en el caso de que se cometa algún delito a través de la telefonía celular.
- Por tanto, la verdadera finalidad de la reforma en cuestión es implícita: identificación plena y certera de los titulares de las líneas de comunicación, a través del Padrón. Donde la coadyuvancia en seguridad y justicia, no es sino una derivación de segundo grado respecto al propósito esencial de la iniciativa
- La finalidad -consistente en el registro y control de las personas a través de un Padrón de líneas telefónicas móviles - que no es constitucionalmente válida, pues no existe en el texto constitucional un valor referido a "controlar y supervisar a los seres humanos", por el contrario, en oposición a estas conductas que se alejan de una concepción humanista y democrática del Estado, se encuentra la protección a los derechos a la privacidad, vida privada, intimidad, identidad y protección de los datos personales.
- En ese sentido, **el Padrón no está vinculado a un objetivo constitucional definido**, puesto que la colaboración con las autoridades en

materia de seguridad y justicia, es contingente, lo que evidencia una ausencia de relación entre medio y fin. Visto así, el Padrón comprende una lógica circular que se autosatisface a sí misma, en tanto que su razón de ser se colma en su existencia. Una tautología que se explica en la creación de un registro de líneas telefónicas móviles cuya causa y consecuencia, es la creación de un registro de líneas telefónicas móviles. Es en ese sentido, que no estamos frente a una finalidad constitucionalmente imperiosa. Es por lo cual, que esta Autoridad considera que la reforma a la LFTR debe ser declarada inválida, en tanto que no conlleva una finalidad constitucionalmente justificada.

- El INAI concluye, que la reforma a la LFTR no cuenta con una finalidad constitucionalmente válida y que, en cualquier caso, dicha medida carece de la debida motivación reforzada que se exige cuando se pueden afectar de manera sustantiva derechos y libertades de las personas.
- Se considera que la medida no es idónea, puesto que evidencia la falta de la relación entre el medio -intervención de los derechos a través de su recopilación, registros, almacenamiento, uso, transferencia, etc.- y el fin, la seguridad pública a través de la colaboración de los delitos de extorsión.
- Otro aspecto que confirma la falta de idoneidad de la reforma, es que conforma una base con la totalidad de los datos de todos los residentes en territorio nacional que cuenten con el servicio de telefonía móvil (finalidad que NO es constitucionalmente válida).
- En tales circunstancias, lejos de que la medida obtenga de algún modo el fin válido, lo que se advierte del propio texto del Dictamen es que no existe evidencia clara y contundente que el registro impacte en la reducción de ese delito. Aunado a que las diversas circunstancias y datos con que se cuentan también dejan de manifiesto que la medida carece de idoneidad.
- En el ordenamiento adjetivo penal se reitera la obligación de los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, de colaborar eficientemente con la autoridad competente para el desahogo de los actos de investigación que exijan las circunstancias del caso, aunado a que, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por la autoridad judicial para operar una orden de intervención de comunicaciones privadas.
- Ya existen otras medidas alternativas que también son idóneas para combatir los delitos de extorsión que se cometen a través de la telefonía móvil, pero que intervienen con menor intensidad en los derechos a la privacidad, intimidad, protección de datos personales, identidad, derechos de la niñez, porque i) la ordena un juez al caso concreto, por lo que será específica en cuanto al dato o información que requiera y no respecto de

todos los datos importantes de las personas, ii) requerirá sólo las actuaciones necesarias respecto de las personas investigadas y no siendo una medida global para toda la población.

- El que se logre inhibir la comisión de delitos no depende de la cantidad de datos personales con los que cuente la autoridad, ni de que cuente con un Padrón con los datos de todos los mexicanos, sino de que en principio las funciones de seguridad pública, persecución e investigación de los delitos, así como administración de justicia, se realicen de forma eficiente y adecuada. De todo lo anterior se concluye, que la medida no es necesaria, en tanto que existen una larga serie de medios igualmente idóneos, y menos lesivos, para lograr el fin perseguido, esto es, colaborar con las autoridades en la inhibición de la comisión del delito de extorsión (a través de la identificación de todas las personas) y, por tanto, es inconstitucional.
- La intervención en el derecho a los datos personales a través de su recopilación, obtención, registro, almacenamiento, uso y transferencia, que ordena la reforma impugnada, impide totalmente la protección de los datos personales así como que los particulares gocen de privacidad e intimidad, en la medida en que se les obliga a dar toda una serie de datos personales que son una radiografía de su vida personal, sin límites ni excepciones. Con lo que, contrario a lo exigido por la jurisprudencia, los derechos quedan totalmente vaciados, intervenidos, y no se observar siquiera un mínimo beneficio, con lo que se concluye que la medida es absolutamente desproporcional.
- La medida que interviene en la protección de los datos biométricos, por un lado, no está directamente encaminada a conseguir la inhibición del delito de extorsión, puesto que, no existe evidencia suficiente que ese tipo de registros y padrones reduzca la incidencia de esos delitos.
- La medida no es la menos restrictiva dentro del abanico de posibilidades para inhibir los delitos, en tanto que existen otras en la propia ley impugnada y en el CNPP que sí lo son y que también se dirigen a combatir la delincuencia. Con lo que, además, al ser datos referidos a la esfera más íntima de las personas, violan el derecho a la intimidad.
- En ese sentido, el INAI considera que al no haber acreditado el cumplimiento del test de proporcionalidad por el cual se determina si una limitación es o no legítima, los artículos de la reforma impugnados, que intervienen en el derecho a la protección de los datos personales incluidos datos sensibles y, por ende, violentan la privacidad y la intimidad, son inconstitucionales y deben declararse inválidos.

En relación con lo anterior, este Colegio coincide plenamente con los argumentos esgrimidos por el máximo órgano garante de la protección de datos personales en

que la emisión del Decreto vulnera el principio de proporcionalidad por las razones que se apuntan a continuación:

- De acuerdo con la LFPDPPP y la LGPDPPSO todo tratamiento de datos debe cumplir con los siguientes requerimientos legales:
    - *Los datos deben ser adecuados, pertinentes y no excesivos en relación con los fines para los que se tratan*. En particular, debe tenerse en cuenta la aplicación de la protección de datos desde el diseño y los requisitos predeterminados, como los campos de entrada limitada (comunicaciones estructuradas) o los controles de calidad automatizados y no automatizados.
    - *El principio de exactitud de los datos.* Los datos deben ser precisos y, cuando sea necesario, mantenerse actualizados. No obstante, el principio de exactitud de los datos debe aplicarse teniendo en cuenta la naturaleza y la finalidad del tratamiento en cuestión. En particular, en los procedimientos judiciales, las declaraciones que contienen datos personales se basan en la percepción subjetiva de las personas físicas y no siempre son verificables. En consecuencia, el requisito de exactitud no debe pertenecer a la exactitud de una declaración, sino simplemente al hecho de que se ha realizado una declaración específica.
    - Debe garantizarse que los datos personales que sean inexactos, incompletos o que ya no estén actualizados no se transmitan ni se pongan a disposición y que se prevean procedimientos para corregir o eliminar los datos inexactos. En particular, se debe tener en cuenta cualquier sistema de clasificación de la información procesada, en cuanto a la confiabilidad de la fuente y en cuanto al nivel de verificación de los hechos.
    - *El principio de conservación de datos.* Los datos no deben conservarse más tiempo del necesario para los fines para los que se procesan. Deben establecerse mecanismos adecuados para el borrado de datos personales; puede ser un período fijo o una revisión periódica de la necesidad de almacenamiento de datos personales (o una combinación de ambos: período máximo fijo y revisión periódica a determinados intervalos). Los datos personales almacenados durante períodos más prolongados para su archivo en el interés público, el uso científico, estadístico o histórico deben estar sujetos a las salvaguardias adecuadas (por ejemplo, con respecto al acceso).
- Existe una falta de legitimación para que el IFT realice el tratamiento de dtos del PANAUT.

- Como hemos dicho, de un lado, la falta de legitimación del IFT convierte al PANAUT en un tratamiento ilícito y la finalidad para el IFT es ilegítima. En consecuencia, el PANAUT en su conjunto debe ser declarado inconstitucional e ilegal por vulnerar el derecho humano de protección de datos personales reconocido en el artículo 16 constitucional sin posibilidad de saneamiento parcial alguno, como se explica a continuación.
- En principio de cuentas reiteramos que el Instituto Federal de Telecomunicaciones carece de las atribuciones normativas para gestionar un registro con fines policiales y de procuración de justicia, los datos en él contenidos son excesivos, no pertinentes y no adecuados en relación con esa finalidad (que a su vez es ilegítima).

- Cuando se tratan datos personales biométricos de un titular para llevar a cabo la identificación unívoca de una persona, estos deben catalogarse como datos personales de naturaleza sensible, esto es así, ya que:
  - La normatividad de desarrollo de los sectores público y privado (La Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la normatividad de desarrollo de las mismas) considera como datos personales sensibles aquellos que afectan la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen o conlleve un riesgo grave para este, como por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas preferencia sexual.
  - La normatividad de desarrollo de los sectores público y privado establece un principio general de prohibición del tratamiento de los datos personales sensibles. Esta prohibición puede excluirse en casos excepcionales previstos en las propias normatividades de desarrollo, siendo la primera de las circunstancias que permite el tratamiento de datos sensibles el consentimiento expreso del titular.
  - Como se advierte, únicamente en circunstancias especiales es posible dar tratamiento a datos personales de naturaleza sensible, ya que es precisamente el mal uso de estos los que puede causar a los titulares afectaciones morales y/o patrimoniales significativas.
  - El tratamiento de datos personales biométricos debe relacionarse con la dignidad humana, la cual es inviolable. Decimos lo anterior, ya que el impacto de lo que la gente percibe como tecnologías de vigilancia en sus vidas puede ser tan significante que afecte su posibilidad de vivir una vida digna. El uso de datos biométricos, como por ejemplo el reconocimiento facial, conlleva que la gente limite sus

derechos y libertades, al evitar acudir a lugares o eventos, o al evitar expresarse libremente, en caso del reconocimiento de voz.

- Existen muchos y diferentes riesgos derivados del tratamiento de datos, en especial los sensibles. Las imprecisiones y los errores inherentes en la recolección y comparación de datos biométricos es uno de ellos. La proporcionalidad, la necesidad y la limitación de uso deben destacar entre los principios rectores.
- La vulneración de seguridad de datos biométricos es especialmente delicada, dado que no es posible cambiar nuestros rasgos fisiológicos, y por lo tanto las consecuencias son más graves.
- Aunque el tratamiento tenga como fundamento la seguridad nacional o una emergencia pública, aún debe evitar violaciones a la dignidad humana. Convertir la cara de las personas en un objeto para la medida y categorización menoscaba la dignidad humana, incluso si no existe una amenaza real de opresión por un estado autoritario. Pero además es que normalmente se prueba en los más vulnerables de la sociedad, los más pobres, las minorías étnicas y los niños. La cosificación del ser humano, sus caras, sus emociones, sus ondas cerebrales, sus movimientos, etc., en particular mediante algoritmos y a gran escala, es en esencia un ataque a la dignidad humana, y aumenta el riesgo real de discriminación.
- Dicho lo anterior, resulta de relevancia especial tener presente para efectos del presente amparo que el tratamiento de datos personales que se pretende llevar a cabo con la creación del PANAUT requiere de una infinidad de datos personales, no solo biométricos, los cuales se utilizarán con el fin primordial de identificar unívocamente a una persona, lo que significa que estos deben considerarse como datos personales sensibles, esto es, como datos personales cuya utilización indebida daría origen a discriminación o un riesgo grave para los titulares de los datos.

- La creación y operación del PANAUT serán sujetos a tratamiento datos personales biométricos que tienen la condición de ser datos personales sensibles.
- Todo tratamiento de categorías de datos personales sensibles que lleva a cabo cualquier sujeto obligado, como lo es el IFT, debe cumplir con los principios y deberes establecidos en la normatividad, sin embargo, para llevar a cabo este es condición necesaria que este se funde en alguna de las siguientes excepciones:
  - El consentimiento expreso del titular o;
  - Alguno de los casos establecidos en el artículo 22 de la LGPDPPSO.

- **El tratamiento de datos personales sensibles exige una justificación concreta y particularmente sólida, basada en motivos distintos de la protección de la seguridad pública contra el terrorismo y los delitos graves de carácter transnacional. Ahora bien, en el caso del PANAUT no existe tal justificación.**

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucionales las disposiciones del Decreto por ser contrarias a los artículos 6o, Apartado A, fracción II, y 16 constitucionales, y 11 de la CADH, 17 del PIDCP, 12 de la DUDH y V de la DADDH, puesto que la medida es desproporcional.

3. Tercer concepto de invalidez

Como tercer concepto de invalidez el INAI indica los artículos 176, 180 bis, 180 ter, 180 Quáter, 180 Quintes (sic), 180 Sextus, así como los Transitorios Tercero, Cuarto y Quinto del Decreto, son contrarios a los artículos 1, 6° y 16 de CPEUM; 5° y 7° del Convenio 108; 1° del Protocolo Adicional al 108; y, 16, 17, 18, 19, 25, 29 y 30 de la LGPDPPSO, al contravenir los principios de *finalidad*, *licitud*, *lealtad, proporcionalidad, responsabilidad* y *seguridad* que rigen el tratamiento de datos personales, así como la seguridad jurídica.

Derivado de esto, en su tercer concepto de invalidez el INAI sostiene quela inclusión del PANAUT, al incluir la obligación de registrar los datos personales del titular de la línea, no se ajusta a ciertos principios rectores del derecho de protección de datos personales por las siguientes razones:

- **Principio de finalidad.** El INAI considera que la creación de padrón de usuarios de telefonía móvil para fines de identificación en una Ley diversa, como lo es la LFTR, es contraria al principio de finalidad, puesto que de conformidad con los artículos 85 y 86 de la LGP, ya existe una base de datos con dicho objeto, como lo es el RENAPO, y por ende, el tratamiento que se propone no podría cumplir con una finalidad concreta, explícita, lícita y legítima conforme el orden jurídico mexicano. Es decir, la finalidad establecida no cumple con las características que se exigen para considerarla válida; en consecuencia, no puede acreditarse el cumplimiento de este principio.
- **Principio de licitud**. El INAI advierte que, con la inclusión de una fracción XLII Bis en el artículo 15, el cual contempla la obligación de instalar, operar, regular y mantener el PANAUT; procurar su buen funcionamiento y el intercambio de información con las autoridades competentes, así como establecer los procedimiento para validar la información que deba

incorporarse al mismo conforme a los sistemas informáticos y procedimientos que establezca para tal efecto, se atribuye una facultad que escapa de su función principal, en tanto que no corresponde al IFT conformar un registro de identidad biométrico. Además, el INAI sostiene que ello genera una transgresión al principio de licitud, pues derivado de las normas que rigen el actuar del sujeto obligado responsable, en este caso, el IFT, no se advierte una norma que lo autorice a instalar una base de datos con fines de identificación de usuarios distintos a los concesionarios, máxime que dicha atribución no es compatible con su objeto.

  - Por lo que respecta a que el tratamiento per se se encuentre apegado a la normativa vigente en materia de datos personales, el incumplimiento de los principios que en este concepto se analizan, así como la violación a los derechos ARCO, lo cual será estudiando en conceptos posteriores, derivan en una violación a las normas que configuran el marco de actuación de las autoridades frente al debido tratamiento de datos. Asimismo, la violación al principio de licitud en esta vertiente, se actualiza dado que no se prevé qué pasará una vez que los concesionarios de telecomunicaciones o sus autorizados entreguen los datos personales al IFT, es decir, no se establece si aquellos deberán conservarlos o eliminarlos de sus registros. Este desconocimiento del destino de los datos, a su vez transgrede el principio de seguridad jurídica, en tanto que dejan a los usuarios de telefonía móvil en un espacio de incertidumbre en donde desconoce quien posee sus datos personales, así como el tratamiento que se les dará.

- **Principio de lealtad**. El INAI considera que el establecimiento del PANAUT con el objeto de verificación de identidad constituye un supuesto que representa riesgos elevados de vulneración tanto por el tipo de información a utilizar, como por el tratamiento automatizado a través de medios de tecnologías de la información, puesto que al establecer una obligación para las concesionarias de telecomunicaciones y sus autorizados, de recabar la información sobre la identidad, datos biométricos y domicilio del usuario, de facto, implica una medida arriesgada que atenta contra la expectativa razonable de privacidad de los usuarios, al permitir que su información de carácter biométrico para fines de identificación personal, pueda ser manipulada por un número elevado de operadores que pueden no que no se justifica conforme a los riesgos inherentes al tratamiento. En ese sentido, tomando en cuenta que los responsables tienen la obligación de brindar un espacio seguro de protección a los titulares de los datos personales, en el caso concreto no se acredita tal obligación, dado que al permitir la manipulación de los datos por parte de un número indefinido de

personas, se crea un escenario en el que el derecho a la protección de datos personales es susceptible de ser vulnerado, por lo que no existe una expectativa razonable de privacidad en favor del titular.

- **Principio de proporcionalidad**. El INAI considera que los artículos 189 y 190, fracciones I, III y IV, del Decreto que reforma la LFTR y por virtud de los cuales, se establecieron obligaciones genéricas a cargo de los concesionarios en la primera de esas materias de proporcionar la información requerida por las autoridades de seguridad, procuración y/o de administración de justicia, así como la obligación de contar permanentemente con los recursos humanos necesarios para cumplir con ese objetivo constituye como una herramienta adicional a las instancias administrativas y/o judiciales para la prevención o persecución de delitos, en razón de que a través de este diseño impuesto a las empresas concesionarias de los servicios de telecomunicaciones podrá emplearse la tecnología destinada a la geolocalización, en tiempo real, de los equipos de comunicación móvil, previa orden judicial. De lo anterior, el INAI precisa:
    - Que se advierte que ya existen mecanismos de apoyo que coadyuvan con la finalidad que hoy se busca con la creación del PANAUT, por lo que la exigencia de entregar datos biométricos, no podría considerarse adecuado y resultan excesivos ya que lejos de cumplir con la finalidad para la cual fue creada, generaría mayores riesgos de vulneración cuya trascendencia se verá reflejada directamente en cada uno de los usuarios de telefonía móvil.
    - El antecedente directo del Padrón Nacional de Usuarios de Telefonía Móvil, consistente en el Registro Nacional de Usuarios de Telefonía Móvil, publicado en el DOF el nueve de febrero de dos mil nueve fue diseñado como una herramienta para combatir el secuestro y la extorsión a través del registro de las líneas telefónicas, asociadas al CURP, que encontraba su fundamento legal en una reforma a la Ley Federal de Telecomunicaciones y que era operado por la Secretaría de Gobernación. El uso de esta base de datos se derogó antes de cumplir tres años en operación, a raíz de la desconfianza y tras confirmarse que era ineficaz para alcanzar los objetivos buscados pues lejos de combatir ciertos delitos, las bases de datos fueron vulneradas y posteriormente, comercializadas. Por ello, tras una dictaminación del antes Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), se ordenó la destrucción de los datos personales que proporcionaron alrededor de 98 millones de usuarios de celulares para el Registro Nacional de Usuarios de Telefonía Móvil. Lo anterior, pues se consideró que el objetivo buscado nunca fue alcanzado y la finalidad para la que fueron ya no subsistía, en

virtud de la creación de la obligación de las empresas de telefonía de coadyuvar con el Ministerio Público Federal en la geolocalización en casos de delincuencia organizada, contra la salud, secuestro, extorsión o amenazas.

- Acontecimientos como éstos, deben generar un indicio de que registros de identidad adicionales al Registro Nacional de Población, cuya finalidad consiste en colaborar en la persecución de delitos, no han sido idóneos y únicamente origina una violación generalizada a los datos personales de los usuarios.
- En un escenario normativo tan desproporcionado como el que se actualiza con el artículo 180 Ter, el INAI considera que se exige un tratamiento excesivo de datos personales, que no se justifican frente a la finalidad y que, por ende, es contrario al principio de proporcionalidad.

- **Principio de responsabilidad**. El INAI indica que, de una lectura detallada de los artículos 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), 180 Sextus, así como, los Transitorios Tercero, Cuarto y Quinto de la LFTR, no se advierte que se contemple el establecimiento de las medidas sustantivas tendentes a garantizar el derecho a la protección de datos personales. Además, se señala que:
  - No debe pasar desapercibido que, en el tratamiento de los datos, se prevé expresamente la intervención de dos sujetos distintos: por un lado, los concesionarios de telecomunicaciones y, en su caso, los autorizados; y por otro lado, el IFT. Dicha circunstancia genera obligaciones extraordinarias en materia de responsabilidad, puesto que el acceso a los datos personales no se concentrará en un solo ente, sino en varios, con lo que el conocimiento, capacitación y actualización en materia de protección de datos, se extiende a un número indefinido de personas, lo cual no está previsto en la reforma.
  - El INAI considera que la omisión de establecer medidas sustantivas dirigidas a la protección de datos personales actualiza una transgresión al principio de responsabilidad, pues es posible que los responsables del tratamiento carezcan de una capacitación adecuada o bien, desconozcan las obligaciones que deben cumplir para garantizar debidamente el derecho.
- **Principio de seguridad**. En relación con este principio el INAI considera que, no debe existir una presunción de seguridad, sino que el responsable debe demostrar que cuenta con todas las medidas para mantener la integridad de la información. Esto genera un deber de utilizar toda su estructura administrativa, tecnológica y técnica para crear un espacio

seguro que evite la pérdida, destrucción, acceso o modificación de los datos que se encuentran a su cargo. Asimismo, el INAI sostiene que:

- Al igual que con el principio de responsabilidad, de una lectura de los nuevos artículos incluidos en la LFTR, no se advierte el establecimiento de medidas de seguridad, o bien, el mandato al IFT para que dichas medidas sean incorporadas en las disposiciones administrativas de carácter general que eventualmente emita para regular el funcionamiento del PANAUT. Por el contrario, el artículo 180 Quintes (sic) contempla la posibilidad de que los concesionarios de telecomunicaciones o los autorizados, en la recopilación de datos personales, utilicen medios remotos siempre que garanticen la veracidad e integridad de la información, lo cual, aumenta el riesgo de que los datos personales sean utilizados para fines distintos.
- La LFTR impone cargas en dos vías: sujetos obligados y particulares como responsables de tratamiento de datos; sin prever que la infraestructura tecnológica y de recursos humanos para su implementación son de mayor costo que el supuesto beneficio buscado ya ubican al usuario en una situación de desventaja de alto riesgo de vulneración y suplantación. Aunado a que los costos implementación, mantenimiento y operación, incluyendo los de conectividad a los servidores del PANAUT, correrán a cargo de los concesionarios y/o autorizados, sin contemplar que ello, no asegura que las dichas medidas cumplan con el principio de responsabilidad.
- No se advierte que en el tratamiento de los datos se establezcan los mecanismos pertinentes con los cuales se daría cumplimiento considerando la gran carga regulatoria que representa para las empresas de telefonía móvil establecer las medidas adecuadas para que sus operadores y/o empleados cumplan a cabalidad con las medidas de seguridad físicas, administrativas y técnicas para dicho tratamiento.

En relación con lo anterior, este Colegio coincide plenamente con los argumentos esgrimidos por el máximo órgano garante de la protección de datos personales en que la emisión del Decreto transgrede los principios de protección de datos personales previstos en la normatividad aplicable por las siguientes razones previamente señaladas en el análisis del primer concepto de invalidez en el apartado relativo a las violaciones al “derecho de protección de datos personales”:

- Los principios, deberes y derechos de protección de datos previstos en la normatividad aplicable configuran al derecho humano a la protección de datos personales como tal, de modo que constituyen su núcleo básico o esencial **y por tanto cualquier fallo o violación de cualquiera de estos principios que**

configuran este derecho humano implica una violación del propio derecho.

- El Decreto resulta inconstitucional toda vez que la creación del PANAUT implica una indubitable transgresión de los principios y deberes de protección de datos previstos en la LFPDPPP y la LGPDPPSO como se expone a continuación:
    - ***Violación al principio de licitud:*** La violación al principio de licitud que configura el derecho a la protección de datos se materializa con la creación del Padrón porque el IFT carece de facultades y atribuciones para instalar, operar, regular y mantener el PANAUT de acuerdo con la finalidad del mismo. Derivado de la propia naturaleza del Padrón ya se advierte la ausencia de habilitación legal al IFT para gestionar dicho registro, pues:
        - El IFT como órgano regulador de los sectores de telecomunicaciones y radiodifusión, no cuenta con ninguna atribución y/o facultad legal que le legitime para el ejercicio de ninguna de las dos funciones señaladas, y
        - La gestión del derecho a la identidad está reservada a la Secretaría de Gobernación, a través del Registro Nacional de Población,[48] como reserva de ley expresa, formal y material, mediante la Ley General de Población cuyo artículo 85 establece que la SEGOB tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero,[49].
        - En definitiva, existe, una ilegitimidad para el IFT de doble vertiente: activa (invasión de la esfera de atribuciones y facultades de la SEGOB) y pasiva (carencia de atribuciones).
        - En virtud de lo anterior, se puede considerar que el hecho de que el legislador federal atribuya al IFT una facultad legal, **contraria a lo establecido por el texto constitucional resulta violatoria de los derechos humanos de legalidad y seguridad jurídica, al constituir una ampliación arbitraria e infundada de las atribuciones constitucionales de dicho órgano regulador con base en lo dispuesto por el artículo 28 de la CPEUM, que además supone una intromisión ilícita en las facultades y competencias de otras autoridades que están legalmente facultadas para las materias que se pretenden atribuir ilícitamente al IFT.**

[48] Artículo 86.- El Registro Nacional de Población tiene como finalidad registrar a cada una de las personas que integran la población del país, con los datos que permitan certificar y acreditar fehacientemente su identidad.
[49] Artículo 85.- La Secretaría de Gobernación tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero.

- ***Violación al principio de finalidad***. El Decreto y la creación del PANAUT violan el principio de finalidad por las siguientes razones:
  - El principio de finalidad regulado tanto en el Convenio 108 como en la LFPDPPP y en la LGPDPPSO establece la obligación de que la obtención y tratamiento de los datos personales deberán sujetarse a finalidades **explícitas, legítimas y determinadas.**
  - En relación con el referido principio, el Convenio 108, en su artículo 5, obliga al Estado Mexicano a establecer medidas para que los datos personales en posesión de sujetos obligados, como lo es el IFT, únicamente sean sujetos a tratamiento cuando **existan fines determinados y legítimos**, prohibiéndose su utilización de forma incompatible con dichos fines. En el presente caso es indudable que el Decreto reclamado vulnera el principio de finalidad y por ende el derecho humano de protección de datos personales en virtud de que:
    - La finalidad explícita por la que se pretende justificar el **Padrón** (colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos cometidos a través de líneas celulares) no resulta adecuada o racional porque no constituye una medida que permita alcanzar el fin perseguido, y es en realidad una finalidad eventual respecto de la **verdadera finalidad** que consiste en la "identificación plena y certera de los titulares de las líneas de comunicación, a través del Padrón" y, solo de forma eventual, en caso de cometerse un delito con la línea celular, emplear esa información para su persecución, por lo que el Padrón tiene un fin primario de registro y control de las personas a través de líneas telefónicas móviles, desde el momento de su adquisición, y
    - El IFT carece de atribuciones o competencias para la realización de este tratamiento, e invade competencias reservadas formal y materialmente por ley.
- ***Violación al principio de proporcionalidad***. Se configura una violación al principio de proporcionalidad previsto en la normatividad vigente en virtud de lo siguiente:
  - El principio de proporcionalidad está previsto en el artículo 5o, inciso c, del Convenio 108, el cual determina que los datos de carácter personal que los Estados recopilen serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado, situación que no se cumple con la

sola creación del PANAUT que ordena recabar datos biométricos sensibles sin que exista una adecuada justificación legal.

- La LGPDPPSO – artículo 25 - y la LFPDPPP – artículo 13-, de forma similar, establecen que **el responsable solo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento,** situación que no se cumple con la sola creación del PANAUT que ordena recabar datos biométricos sensibles sin que exista una adecuada justificación legal.
- El Decreto **vulnera el principio de proporcionalidad** y por ende el derecho humano de protección de datos personales en virtud de que, como se demostrará a continuación:
    - Los datos personales objeto del tratamiento del Padrón **son excesivos** para la finalidad de colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos cometidos a través de líneas celulares, ya que los datos personales objeto del tratamiento del Padrón son de una naturaleza tendiente a crear un registro de identidad que permiten certificar y acreditar fehacientemente la identidad de los ciudadanos, finalidad que no es compatible con la finalidad para la cual fue creado el Padrón.
    - Obliga al tratamiento de **datos personales biométricos**, mismos que constituyen datos personales sensibles sin que exista legitimación alguna que lo permita ni sea proporcional su tratamiento.
    - Existe una **conservación injustificada** de los datos personales de los usuarios sin limitación de los periodos de retención. En particular, para el tratamiento de datos personales sensibles, el responsable del tratamiento está obligado a realizar esfuerzos razonables para limitar el periodo de tratamiento al mínimo indispensable.
    - En particular, **no se permite la supresión** de los datos cuando los usuarios dan de baja su línea celular, sino que, sin justificación alguna, se mantendrán durante 6 meses.

- ***Violación al principio de responsabilidad***. La normatividad aplicable en materia de protección de datos personales exige el cumplimiento de una serie de acciones demostrables tendientes a demostrar que el tratamiento de datos que realice el responsable conforme a la normatividad, y, concretamente **en cumplimiento del principio de responsabilidad, previsto en los artículos 14 de la**

LFPDPPP y 74 de la LGPDPPSO, que el responsable del tratamiento realice una **Evaluación de Impacto en la Protección de Datos Personales (en adelante "EIPDP")** cuando exista la probabilidad de que, por su naturaleza, alcance o fines, las operaciones de tratamiento entrañen un alto riesgo para los derechos y las libertades de los titulares de datos personales. Es decir, cuando exista un tratamiento intensivo o relevante de datos personales. En este contexto, se debe recordar que la EIPD:

- Tiene que realizarse de manera previa al tratamiento que se "pretenda poner en operación" que suponga un tratamiento intensivo. Así expresamente el articulo 77 de la LGPDPPSO y el artículo 23 de las Disposiciones EIPDP indican que, los sujetos obligados que realicen una EIPDP, deberán presentarla ante el INAI (o los organismos garantes) cuando menos **treinta días antes** a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, a efecto de que se emita el dictamen correspondiente en los treinta días siguientes (ex art. 78 LGPDPPSO).
- Uno de sus objetivos principales es identificar y describir los altos riesgos potenciales y probables que entrañen los tratamientos intensivos o relevantes de datos personales.
- Se basa en el contraste entre la situación de partida y lo que ocurre una vez que el tratamiento tenga lugar. Ese contraste busca revelar los cambios que se pueden atribuir al tratamiento realizado.
- Derivado de las conclusiones en esa evaluación habrá que decidir si ese tratamiento se puede llevar a cabo, y, en su caso, con qué medidas de seguridad.
- Tal y como el mismo Dictamen de reforma a la LFTR del 16 de abril de 2021 reconoce: *(…)* ***v. Será necesario realizar una evaluación de impacto a la protección de datos personales****, mismo que implica la vulneración de los datos que son confidenciales"*

- El simple hecho de que el Legislador haya sido omiso en realizar una apreciación de proporcionalidad (*test de proporcionalidad*) respecto de la creación del PANAUT en relación con la restricción al derecho humano a la protección de datos personales e instruir al IFT como órgano responsable del tratamiento de datos relativos al PANAUT llevar a cabo una EIPDP, **es violatorio del**

derecho humano de protección de datos personales por incumplimiento al principio de responsabilidad.

- ***Violación al deber de seguridad***. En relación con la violación al deber de seguridad es importante tomar en cuenta lo siguiente:
  - Tanto en la LFPDPPP como en la LGPDPPSO la obligación de seguridad se regula como un deber, y por lo tanto, como una obligación proactiva, preventiva y demostrable para todos los responsables del tratamiento sean estos entes públicos o privados, obligándoles dicho deber a establecer y mantener diversos controles de seguridad administrativos, físicos y técnicos para evitar que la confidencialidad, integridad y disponibilidad de la información se vean comprometidas.
  - No puede obviarse que los costos de implementar medidas de seguridad como las que se requiere para garantizar la seguridad de los datos personales que son objeto del tratamiento en el PANAUT son significativos, aunado a los recursos humanos requeridos para su implementación. Ahora bien, en el presente caso existe evidencia objetiva **en cuanto a que el cumplimiento de este deber de seguridad resulta de imposible cumplimiento tanto para el IFT como para los concesionarios**.
  - De lo anterior se advierte que el IFT ha reconocido públicamente **que le es imposible destinar recurso alguno a la instalación, operación, regulación y mantenimiento del PANAUT, lo que significa que una de las bases de datos más sensibles e importantes del país, en cuanto a que un mal uso de los datos personales ahí contenidos tendría como consecuencia afectaciones irreparables para los titulares de los datos personales, no contendrá control de seguridad alguno, ya que no existe presupuesto para ello.**
  - En relación con lo anterior no puede pasar desapercibido que los datos personales contenidos en el PANAUT tendrán un valor en el mercado extremadamente alto, por lo que dicha base de datos será susceptible de múltiples ataques en materia de ciberseguridad, en especial si tenemos como referencia los siguientes sucesos que se han presentado, en los últimos años.

En relación con lo anterior, este Colegio coincide en que la emisión del Decreto viola el **principio de seguridad jurídica** por las razones:

- La información que formará parte del PANAUT refiere a datos de: i) usuarios de telefonía, ii) titulares de una línea telefónica y iii) usuarios

titulares. Lo anterior es contrario al propio contenido del artículo 180 Bis y confuso siendo que el contenido de los artículos del Decreto refieren de forma indistinta a titulares y usuarios omitiendo considerar que puede tratarse de personas diferentes.

- Esta situación genera incertidumbre jurídica puesto que los artículos en comento no definen a quién va dirigida la obligación de proporcionar los datos. La norma jurídica está compuesta en su estructura lógica por el supuesto que refiere a la conducta o estado de cosas regulada, el nexo verbal mediante el que se verifica el supuesto y la sanción que refiere a la consecuencia jurídica prevista.[50] En todos estos elementos mínimos debe estar definido el sujeto normativo. Por tanto, la precisión de quién es el **sujeto obligado** es un elemento que necesariamente debe estar presente desde la configuración de la norma como uno de sus elementos estructurales.
- Por tanto, el determinar a quién va dirigida una norma no es un elemento susceptible de posterior desarrollo en un Lineamiento o en una reglamentación sino que constituye un elemento estructural a la formulación de la norma que debe ser determinada desde la Ley.
- Por lo anteriormente expuesto los artículos 180 Bis, 180 Ter, 180 Quáter y 180 Quintes así como artículos Cuarto y Quinto transitorios del Decreto carecen de los elementos necesarios para determinar el alcance de las normas que conforman, dejando al gobernado en incertidumbre jurídica en transgresión a los artículos 14 y 16 de la CPEUM en transgresión al derecho de seguridad jurídica y principio de legalidad.
- Los artículos 180 Ter, 180 Quáter, 180 Quintes y el artículo Cuarto transitorio del Decreto transgreden el derecho a la seguridad jurídica y al principio de legalidad contenidos en los artículos 14 y 16 de la Constitución Federal en tanto obligan a dos sujetos a la entrega de datos biométrico: al representante legal de la persona moral titular de la línea telefónica, y al usuario de una línea telefónica. Por otra parte, la LFTR deja en total indefinición cuáles son los datos biométricos que se van a recabar.
- Respecto de los datos biométricos la LFTR no establece a qué se refiere con datos biométricos, dejando al titular de la línea telefónica en un estado de incertidumbre sobre la obligación que se lo impone. Esta incertidumbre trasciende además para el usuario de la línea telefónica, así como para los representantes legales de las personas morales. Esta situación se repite en la fracción VI del artículo 180 Ter de la LFTR que también se refiere a los “datos biométricos” del usuario, sin especificar

[50] Carla Huerta Ochoa, Conflictos normativos, editado por el Instituto de Investigaciones Jurídicas de la UNAM, IMPRESO EL 3 DE AGOSTO DE 2007, Estado de México, página 21

cuáles son serán los que se deben proporcionar como condición para recibir el servicio de telefonía móvil.

- De esta forma, en los términos que está redactado el artículo 180 Ter se podrían requerir desde huellas digitales, iris, rostro, retina, voz, piel, el ADN, etcétera, sin que la LFTR establezca limitación alguna, o bien, justificación sobre las razones porque las que se solicitan dichos datos de naturaleza sensible, lo que deja en estado de incertidumbre jurídica al titular y usuario de las líneas de telefonía móvil, e incluso a los representantes legales de las personas morales.
- En este sentido, para cumplir con los principios de seguridad jurídica y de legalidad, era necesario que el alcance de esta obligación quedara definida desde el texto legal, aportando además los elementos que permitieran justificar que dichos datos debían ser recabados. Más aun, cuando de acuerdo con el artículo 180 Bis de la LFTR el único fin del PANAUT "es el de colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos en los términos de las disposiciones jurídicas aplicables." Por lo que los datos biométricos que sirven para dicha finalidad en todo caso debieron ser definidos por los legisladores.
- El artículo 180 Séptimus del Decreto señala que las autoridades de seguridad de procuración y administración de justicia podrán acceder a la información del PANAUT.
- El referido artículo señala de manera genérica y en violación a los principios de seguridad jurídica y de legalidad, quiénes podrán acceder a la información del PANAUT y cómo podrán acceder a ella. No obstante la relevancia de ambos temas, el legislador no definió quiénes serán las autoridades que podrán acceder a la información. Si bien el artículo dispone que podrán acceder a los datos del PANAUT las autoridades "de seguridad de procuración y administración de justicia" que tengan dentro de sus atribuciones la facultad expresa para requerir al IFT los datos del PANAUT, no las limita en ningún sentido. Esto debido a que no se establece un nivel jerárquico para que solo algunas autoridades de procuración de justicia accedan a esta información, ni se establece alguna otra limitación que acote a las autoridades.
- Esta situación genera incertidumbre en los usuarios de telefonía y titulares de una línea telefónica debido a que se les está obligando a proporcionar información sin conocer quién tendrá acceso a ella, lo que contraviene los derechos de protección de datos personales y a la autodeterminación informativa.
- Aunado a lo anterior, desde la propia ley no se establecen contrapesos a las facultades de las autoridades que permitan garantizar los derechos

de los usuarios y titulares de una línea. Eso así ya que aun cuando los datos del PANAUT son datos sensibles no se establece la obligación de las autoridades de contar con autorización judicial de forma previa al acceso a los datos del PANAUT.

- Se pretende delegar en disposiciones administrativas emitidas por el IFT las normas que regulen el tratamiento de los datos personales y biométricos que se encontrarán en el PANAUT. Lo anterior genera incertidumbre jurídica y contraviene el principio de legalidad en tanto que el IFT no es la autoridad competente para determinar la regulación aplicable al tratamiento de datos personales.

En ese sentido, este Colegio coincide plenamente con el INAI en que la incorporación de un padrón de usuarios de telefonía móvil a la LFTR contraviene los principios de finalidad, licitud, lealtad, proporcionalidad y responsabilidad, así como el deber de seguridad establecidos en LGPDPPSO, así como en el Convenio 108 y su Protocolo Adicional, por lo que su contenido debe ser declarado inconstitucional.

4. Cuarto concepto de invalidez

Como cuarto concepto de invalidez el INAI indica los artículos 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), 180 Sextus, así como los Transitorios Tercero, Cuarto y Quinto de la LFTR, son contrarios a los artículos 1, 6° y 16 de la CPEUM; 5° y 7° del Convenio 108; 1° del Protocolo Adicional al Convenio 108; y, 16, 17, 18, 19, 25, 29 y 30 de la LGPDPPSO, al no brindar un protección reforzada a datos biométricos cuya naturaleza es la de un dato personal sensible y violar el principio de seguridad jurídica.

Derivado de esto, en su cuarto concepto de invalidez el INAI sostiene que tomando en cuenta que se está ante datos de carácter sensible, no se establecen obligaciones complementarias de protección, incluso, no se hace referencia a ningún deber de salvaguarda de los datos que se pretenden recopilar, y, entre otras cosas precisa que:

- Al tratarse de una intervención sobre derechos humanos, resultaba necesario que el Congreso de la Unión, en ejercicio de las facultades consagradas en el artículo 73, fracciones XXIX-O y XXIX-S, definiera de forma precisa el alcance de la afectación, señalando los datos biométricos a ser recabados.
- El legislador federal dejó esa determinación a una autoridad que no está facultada constitucionalmente para ello, pues el artículo 180 Ter, fracción VI, de la LFTR dispone que los datos biométricos a recabar se

determinarán en las disposiciones administrativas de carácter general que al efecto emita el IFT donde se definirá ese aspecto.

- El INAI considera que, tomando en cuenta que los datos biométricos tienen el carácter de datos sensible y que por ello, deben ir acompañados de un nivel de protección reforzado por parte del responsable, es que el Capítulo I bis debe ser declarado inconstitucional, en tanto que el legislador ordinario no previó un marco jurídico adecuado y reforzado que permita generar en el titular una actitud de confianza respecto del tratamiento de sus datos.

En relación con lo anterior, este Colegio coincide en que la emisión del Decreto viola el principio de seguridad jurídica por las razones siguientes:

- Respecto de los datos biométricos la LFTR no establece a qué se refiere con datos biométricos, dejando al titular de la línea telefónica en un estado de incertidumbre sobre la obligación que se lo impone. Esta incertidumbre trasciende además para el usuario de la línea telefónica, así como para los representantes legales de las personas morales. Esta situación se repite en la fracción VI del artículo 180 Ter de la LFTR que también se refiere a los “datos biométricos” del usuario, sin especificar cuáles son serán los que se deben proporcionar como condición para recibir el servicio de telefonía móvil.
- De esta forma, en los términos que está redactado el artículo 180 Ter se podrían requerir desde huellas digitales, iris, rostro, retina, voz, piel, el ADN, etcétera, sin que la LFTR establezca limitación alguna, o bien, justificación sobre las razones porque las que se solicitan dichos datos de naturaleza sensible, lo que deja en estado de incertidumbre jurídica al titular y usuario de las líneas de telefonía móvil, e incluso a los representantes legales de las personas morales.
- En este sentido, para cumplir con los principios de seguridad jurídica y de legalidad, era necesario que el alcance de esta obligación quedara definida desde el texto legal, aportando además los elementos que permitieran justificar que dichos datos debían ser recabados. Más aun, cuando de acuerdo con el artículo 180 Bis de la LFTR el único fin del PANAUT “es el de colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos en los términos de las disposiciones jurídicas aplicables.” Por lo que los datos biométricos que sirven para dicha finalidad en todo caso debieron ser definidos por los legisladores.

En ese sentido, este Colegio coincide plenamente con el INAI en que los artículos 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), 180 Sextus, así como los Transitorios Tercero, Cuarto y Quinto de la LFTR, son contrarios a los artículos 1, 6° y 16 de la CPEUM; 5° y 7° del Convenio 108; 1° del Protocolo Adicional al

Convenio 108; y, 16, 17, 18, 19, 25, 29 y 30 de la LGPDPPSO, al no brindar un protección reforzada a datos biométricos cuya naturaleza es la de un dato personal sensible y violar el principio de seguridad jurídica, por lo que su contenido debe ser declarado inconstitucional.

5. Quinto concepto de invalidez

Como quinto concepto de invalidez el INAI indica los artículos 180 Quintes (sic) y 180 Septimus del Decreto impugnado, son contrarios a lo dispuesto por el artículo 16 de la CPEUM y lo previsto por la LGPDPPSO al incluir mecanismos distintos y restrictivos para ejercer los derechos de *acceso, rectificación, cancelación* y *oposición* de datos personales.

De acuerdo con lo anterior, el INAI sostiene lo siguiente:

- Se actualiza una omisión legislativa de naturaleza parcial al no señalar los requisitos de presentación de la solicitud, plazos de respuesta y de actuación, así como, medios de impugnación específicos en caso de inconformidad del titular debido la actuación del sujeto obligado responsable.
- Dicho criterio sustenta la premisa de que el Congreso de la Unión no puede dejar de incorporar elementos esenciales para ejercer o defender un derecho, sobre todo cuando existe una LGPDPPSO que los señala expresamente y que, por tanto, deben ser replicados en las legislaciones federales y locales. La omisión de incorporarlos, genera un ambiente de inseguridad jurídica, pues el particular no conoce el marco regulatorio completo que acompaña al derecho de protección de datos personales del cual es titular.
- En segundo lugar, se actualiza una contradicción clara entre el derecho de acceso a datos personales reconocido por los artículos 8, inciso a, del Convenio 108 y 43 y 44 de la LGPDPPSO. Lo anterior es así, pues el numeral 180 Septimus limita el acceso únicamente al número o números de celular asociados con el titular, sin tener la posibilidad de conocer la totalidad de datos personales que están vinculados a él.
- Finalmente, se transgreden el derecho de cancelación de datos personales reconocido por los artículos 8, inciso c, del Convenio 108 y 46 de la LGPDPPSO, pues si bien se reconoce que el titular de los datos tiene a su alcance la posibilidad de cancelar un número de línea que no reconozca como suyo, igualmente se prevé que esa cancelación no implica la eliminación del registro correspondiente, aunado a que el registro de la línea asociado al solicitante de la cancelación, permanecerá vigente por el plazo de seis meses. Especialmente este supuesto genera una afectación

que debe llamar la atención, pues la obligación de conservar el registro posterior a la solicitud de cancelación, origina una presunción sobre la creación de bases de datos accesorias en la cuales se desconoce si habrá un historial que continúe vinculando el dato con un particular.

- Una norma que tenga como objeto obstaculizar el ejercicio de estos derechos tendrá dos consecuencias de naturaleza distinta: i) por un lado, una de naturaleza práctica, la cual implica que el derecho a la protección de datos personales se volvería nugatorio; y, ii) por otro lado, una de naturaleza jurídica –que es la que para esta demanda interesa-, en la que esos obstáculos al no ser acordes con el parámetro de regularidad constitucional, deben ser declarados inconstitucionales, a fin de evitar un daño irreparable en la esfera de los titulares de datos personales.

En relación con lo anterior, este Colegio coincide plenamente con los argumentos esgrimidos por el máximo órgano garante de la protección de datos personales en que la emisión del Decreto vulnera el ejercicio de los Derechos ARCO de los Titulares por las siguientes razones:

- El derecho a la protección de datos personales es un derecho humano que dota a los titulares de datos personales de un haz de facultades para decidir sobre las condiciones bajo las cuales consienten el tratamiento de sus datos personales y tener control de su información personal. Como decíamos, en nuestro ordenamiento jurídico dicho reconocimiento legal se deriva de lo previsto por el párrafo segundo del artículo 16 de la CPEUM que indica que "*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*". Para que este derecho tenga concreción práctica, la normatividad aplicable a la protección de datos personales en los sectores público y privado prevé ciertos mecanismos jurídicos para que las personas controlen su información personal, demanden que su información sea tratada de forma lícita y a su vez los entes responsables del tratamiento cumplan con sus obligaciones legales.
- La LGPDPPSO y la LFPDPPP desarrollan las reglas para su tramitación y ejercicio ante el responsable del tratamiento. Dichas prerrogativas se conocen con el acrónimo de "Derechos ARCO" y tienen un contenido particular que los distingue entre sí. En el sector público, además la LGPDPPSO establece otra prerrogativa adicional conocida como "derecho de portabilidad", por lo que, en el sector público además se incorpora este derecho a los tradicionales Derechos ARCO para referirse a esta serie de derechos como "Derechos ARCOP".

- El articulo 8o del Convenio 108 contempla garantías complementarias para el titular de los datos que básicamente consisten en el ejercicio de los referidos derechos: I) obtener sin demora la confirmación de la existencia o no de datos de carácter personal que le conciernan; y, II) obtener la rectificación de los datos o el borrado de estos cuando se hayan tratado con infracción a las disposiciones del derecho interno.
- Son los derechos ARCO los que dotan a los titulares de un conjunto de facultades para mantener el control sobre su información personal, que van desde el derecho a saber quién posee sus datos personales, los usos a los que se están sometiendo los mismos, hasta el poder de oponerse a su posesión y uso concreto, y en caso de que el tratamiento no se realice conforme a derecho, solicitar la eliminación de los mismos.
- Como decíamos, los cuatro derechos –Derechos ARCO- encuentran un reconocimiento convencional, constitucional y legal (ley general), dentro de cual se desarrolla su contenido y se detallan las reglas para su ejercicio ante el responsable del tratamiento, otorgando expresamente a los titulares de los datos personales los derechos a acceder, rectificar y cancelar su información personal en posesión de terceros, así como a oponerse a su uso, y en el sector público incluso se otorga la posibilidad de ejercer la portabilidad de dichos datos hacia otro responsable. A grandes rasgos los Derechos ARCOP son los siguientes:
    - ***Acceso***. El derecho de acceso se encuentra comprendido dentro de la gama de derechos que garantizan la protección a los datos personales de sus titulares; tiene por objeto que el titular pueda conocer qué datos personales suyos son objeto de tratamiento por parte del responsable, las finalidades para los cuales fueron recabados, así como las generalidades de dicho tratamiento a través del aviso de privacidad. Así, podemos decir que el derecho de acceso es una herramienta eficaz que tienen los titulares para evitar que los responsables lleven a cabo, sin su conocimiento, una acumulación de sus datos personales y darles usos distintos a los acordados entre las partes que conllevaría a que el titular perdiera control sobre su información.
    - ***Rectificación***. Derecho de los titulares para solicitar al responsable que modifique los datos personales que resulten ser inexactos o incompletos, esto es, es la posibilidad que tiene el titular de exigir al responsable cumplir con el principio de calidad de los datos, dando lugar a que el tratamiento esté apegado a la realidad.
    - ***Cancelación***. Es el derecho que tienen los titulares para excluir del tratamiento sus datos personales, ya sea por ser inexactos, por no querer que sean sujetos de tratamiento o bien porque considere que

están siendo tratados en contravención a los principios y deberes consagrados en la normatividad. Este derecho puede solicitarse respecto de la totalidad de los datos personales del titular, o bien específicamente respecto de alguno de ellos e implica el cese en el tratamiento por parte del responsable, a partir de un bloqueo de los mismos y su posterior supresión.

- ***Oposición***. habilita al titular para que pueda oponerse al tratamiento de sus datos personales para aquellas finalidades que no resulten necesarias para el cumplimiento de la relación jurídica principal entre el responsable y el titular. La LGPDPPSO especifica que la oposición procederá cuando siendo lícito el tratamiento, el mismo deba cesar para evitar que su persistencia le cause un perjuicio o el titular requiera manifestar su oposición para fines específicos y lo hace extensible a los tratamientos automatizados de datos personales en determinadas circunstancias.
- ***Portabilidad***. El derecho a la portabilidad permite a los titulares recibir los datos personales proporcionados a un responsable en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento. Su finalidad es brindar a los titulares mayor control sobre la información personal que les concierne, facilitando su habilidad para mover, copiar o transmitir sus datos personales con facilidad de un entorno tecnológico a otro.

- En lo que respecta a la función de los Derechos ARCOP, de conformidad con la normatividad vigente, se puede advertir que estos tienen una doble utilidad:
  - Otorgan al titular el poder de decisión y control sobre la información que le concierne y, en consecuencia, permiten garantizar su derecho a la protección de sus datos personales.
  - Actúan como complemento del mandato del responsable de cumplir con las obligaciones que le son impuestas en la LFPDPPP y la LGPDPPSO, permitiéndole identificar aquellos casos en los que el tratamiento pudiera no ajustarse a la normatividad aplicable.
- En relación con los referidos Derechos ARCO, el Poder Judicial de la Federación en la tesis I.10o.A.5 CS (10a.) localizable en la Gaceta del Semanario Judicial de la Federación, Libro 70, Septiembre de 2019, Tomo III, página 2199 ha señalado lo siguiente:

PROTECCIÓN DE DATOS PERSONALES. CONSTITUYE UN DERECHO VINCULADO CON LA SALVAGUARDA DE OTROS DERECHOS FUNDAMENTALES INHERENTES AL SER HUMANO.

> *El párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce los denominados derechos ARCO, relativos al acceso, rectificación, cancelación y oposición de datos personales, como un medio para garantizar el derecho de los individuos a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de la sociedad, y la posibilidad de exigir su cumplimiento a las autoridades y particulares que conocen, usan o difunden dicha información. Así, dichas prerrogativas constituyen el derecho a la protección de los datos personales, como un medio de salvaguarda de otros derechos fundamentales previstos en la propia Constitución y en los tratados internacionales de los que México es Parte, conforme a los cuales, el Estado tiene la obligación de garantizar y proteger el derecho de todo individuo a no ser interferido o molestado por terceros o por una autoridad, en ningún aspecto de su persona –vida privada–, entre los que se encuentra el relativo a la forma en que se ve a sí mismo y como se proyecta a los demás –honor–, así como de aquellos que corresponden a los extremos más personales de la vida y del entorno familiar –intimidad–, o que permiten el desarrollo integral de su personalidad como ser humano –dignidad humana–.*

- De lo señalado en la anterior tesis, se advierte que los Derechos ARCO fungen como un medio de salvaguarda de otros derechos fundamentales previstos en la propia Constitución y en los tratados internacionales de los que México es parte como la vida privada, el honor, la intimidad y la dignidad humana.
- La existencia de una normatividad que obligue al tratamiento de datos personales que no garantice a los titulares de quienes se tratan sus datos personales el ejercicio completo de sus derechos ARCO sería inconstitucional por vulnerar el derecho humano de protección de datos personales reconocido en el párrafo segundo del artículo 16 constitucional.
- El artículo 180 Quintes de la LFTR concede al usuario la posibilidad de solicitar la baja de su línea celular del PANAUT cuando esta no lo reconozca como propia, sin embargo, la referida disposición **es contundente al señalar que la baja de la línea no implica la eliminación del registro correspondiente dando lugar a una conservación perpetua e indefinida de datos personales y sin ninguna garantía de seguridad.**
- De acuerdo con la LFPDPPP y la LGPDPPSO el derecho de cancelación es el derecho que tienen los titulares para excluir del tratamiento sus datos personales, ya sea por ser inexactos, por no querer que sean sujetos de tratamiento o bien porque considere que están siendo tratados en

contravención a los principios y deberes consagrados en la normatividad. **La cancelación**, una vez concedida, y cuando no exista un periodo de bloqueo por no existir una disposición legal que fije un plazo de prescripción, **conlleva la supresión / borrado inmediato de los datos personales**. No cumplir con el borrado inmediato de los datos personales una vez ejercido un derecho de cancelación implicaría que el responsable del tratamiento sigue dando tratamiento a los datos personales en contravención al derecho humano de protección de datos personales, por la inexistencia de una finalidad y una base de legitimación que le legitime a ello.

- Al respecto, debemos recordar que el PANAUT no se limita al registro de los usuarios de las líneas telefónicas a sus números de líneas celulares, sino que dicho registro implica la entrega **de muchos otros datos personales**, como lo son los datos biométricos de los usuarios. En este sentido, tampoco debe olvidarse que el registro de dichos datos personales **está condicionado a que seas un usuario de una línea celular** – lo que se busca es la eventual inhibición de delitos cometidos a través de estas - por lo que en caso de que cualquier persona deje de ser un usuario de una línea celular, **no tendría justificación alguna que dicha persona - no usuaria de una línea celular - esté registrada en el PANAUT**. Esto es, la supuesta finalidad por la cual se crea el PANAUT es para combatir exclusivamente aquellos ilícitos que se cometen mediante el uso de una línea celular, por lo que la inexistencia de ser un usuario de una línea celular tendría como consecuencia lógica que no debas ser registrado y/o permanecer registrado en el PANAUT. Sin embargo, contrario a dicho razonamiento, la disposición 180 Quintes señala: ***"la baja de un número de línea telefónica móvil en el Padrón Nacional de Usuarios de Telefonía Móvil no implica la eliminación del registro correspondiente".*** Esto significa que el IFT seguirá tratando los datos personales de los titulares de datos personales incluso cuando estos no sean usuarios de una línea celular, lo que se traduce en una violación flagrante del derecho humano de protección de datos personales por no existir una finalidad que justifique el tratamiento de los datos personales.
- Por su parte, el artículo 180 Septimus limita injustificadamente el derecho de acceso de los titulares en virtud de que este solo permite acceder a los números telefónicos que le están asociados, y no así al resto de los datos personales que están registrados en el PANAUT, como lo son los datos biométricos de los usuarios. El referido artículo 180 Septimus en la parte que interesa señala: "El Instituto habilitará los mecanismos de consulta para que cualquier persona física o moral que acredite fehacientemente su

personalidad **pueda consultar únicamente los números telefónicos que le están asociados.**"

- Por otro lado, tanto la LFPDPPP como la LGPDPPSO establecen que el ejercicio de **derechos ARCO debe ser sencillo y gratuito**. Respecto de la sencillez en el procedimiento de su ejercicio, se puede destacar que esta significa que los medios que el responsable implemente para la atención de los derechos de los titulares, ya sean remotos, locales, o de comunicación electrónica, u otros que considere pertinentes, permitan el ejercicio de los Derechos ARCO, no limiten su ejercicio ni impliquen dificultades para su tramitación. También en aras de no vulnerar este derecho es necesario que estén regulados los requisitos de presentación de la solicitud, los plazos de respuesta y los plazos de actuación en caso de que la solicitud sea procedente, ya que de no existir estos no puede existir una garantía efectiva del derecho.
- Lo anterior implica que cualquier Ley que contemple cualquier tratamiento de datos personales, como lo es la LFTR en lo que respecta a la instalación y operación del PANAUT, debe incorporar los parámetros antes señalados y no contradecirlos; de lo contrario, esos tratamientos de datos personales serán ilícitos, y las normas que obligan a estos inconstitucionales.
- Del contenido de los artículos 180 Quintes y 180 Septimus de la LFTR que son precisamente las disposiciones que regulan el ejercicio de los derechos de cancelación y oposición de los titulares se advierte que carecen de los parámetros necesarios para poder garantizar el debido ejercicio y atención de dichos derechos, ya que:
    - No fijan medio para su ejercicio;
    - No establecen plazos de respuesta;
    - No fijan un procedimiento para su atención;
    - No fijan mecanismos de acreditación de identidad.
    - No establecen medios de impugnación en caso de que el titular no esté satisfecho con la atención de su derecho;
- Una norma que tenga como objeto obstaculizar el ejercicio los derechos ARCO, como lo son los artículos 180 Quintes y 180 Septimus tiene dos consecuencias innegables:
    - El derecho humano de protección de datos personales se convierte en algo ilusorio;
    - Incumplen con el parámetro de regularidad constitucional, y causarán un daño irreparable en la esfera de los titulares de datos personales.
- En síntesis, insistimos que para que se pueda garantizar el derecho humano de protección de datos personales es condición necesaria que los titulares de los datos personales dispongan de garantías suficientes para la

protección eficaz de sus datos personales frente a los riesgos de abusos y frente a cualquier posible acceso o uso ilícitos de los mismos, mediante el ejercicio de sus derechos ARCO. Para ello es imprescindible que existan **normas claras y precisas que regulen el alcance y ejercicio de estos derechos, de manera que las personas cuyos datos sean objeto de tratamiento dispongan de garantías suficientes para la protección eficaz de sus datos personales frente a los riesgos de abusos y frente a cualquier posible acceso o uso ilícitos de los mismos.**

En ese sentido, este Colegio coincide con el INAI en que los artículos 180 Quintes (sic) y 180 Septimus, al contemplar derechos ARCO que se ejercen de manera distinta y limitada a los previsto por la LGPDPPSO, deben ser declarados inconstitucionales al no ser acordes con el parámetro de regularidad constitucional.

6. Sexto concepto de invalidez

Como sexto concepto de invalidez el INAI indica los artículos 15, fracción XLII bis, 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), 180 Sextus, 180 Septimus, Primero, Segundo, Tercero, Cuarto y Quinto Transitorios del Decreto impugnado, son violatorios de los artículos 6o, Apartado A, fracción VIII, primer y segundo párrafos, 16, segundo párrafo, 28, párrafo quince y fracciones XXIX-O y XXIX-S, del artículo 73 de la CPEUM, en tanto que, contrario a lo establecido en los artículos en cita, faculta al IFT a emitir disposiciones en materia de protección de datos personales, lo que viola estos derechos, invadiendo, además con ello, las facultades constitucionales que tiene el INAI.

En relación con lo anterior, el INAI sostiene lo siguiente:

- El IFT no tiene facultades para emitir disposiciones en materia de datos personales, pues en términos de lo dispuesto por artículo 28 constitucional, tiene a su cargo la regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de radiodifusión y telecomunicaciones, así como del acceso a infraestructura activa, pasiva y otros insumos esenciales, garantizando lo establecido en los artículos 6o. y 7o. de la CPEUM. Se constituye, igualmente, como la autoridad en materia de competencia económica de los sectores de radiodifusión y telecomunicaciones.
- Si bien el IFT cuenta con facultades para emitir disposiciones de carácter general, tal facultad regulatoria sólo se habilita respecto al ámbito de competencia que la CPEUM le señala, a saber, uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los

servicios de radiodifusión y telecomunicaciones, así como del acceso a infraestructura activa, pasiva y otros insumos esenciales y, en materia de competencia económica de los sectores de radiodifusión y telecomunicaciones.

- Los artículos impugnados violan lo establecido en el artículo 28 constitucional, párrafos quince y dieciséis, en tanto facultan al IFT a emitir disposiciones de carácter general en materia de datos personales, lo que se encuentra fuera de su competencia constitucional, de ahí que se desborden las atribuciones que tiene encomendadas en el artículo fundamental en cita.
- En segundo lugar, se invaden y violentan las facultades que este organismo garante tiene en la materia de datos personales y, por ende, se viola también la garantía institucional de autonomía.
- El IFT no tiene facultades para emitir regulación en materia de datos personales, en tanto que no es la materia de su competencia constitucional, en este sentido el órgano constitucional autónomo a quien le corresponde tal facultad -emitir regulación en materia de datos personales- es al INAI. Esto es así, pues tal facultad es inherente a su naturaleza de órgano constitucional autónomo.
- En todo caso, sería al INAI a quien le correspondería emitir la regulación relacionada y/o vinculada con el ejercicio del derecho de protección de datos personales. Es así, ya que en términos de los dispuesto por la CPEUM, es el órgano del Estado mexicano especializado, técnico y garante del ese derecho fundamental.
- Se considera que existe una transgresión al principio de reserva de Ley, de manera específica por cuanto hace al mandato establecido en las fracciones XXIX-O y XXIX-S, del artículo 73 de la CPEUM.
- El habilitar a un órgano del Estado mexicano con una facultad para emitir disposiciones administrativas de carácter general, respecto de una materia para la cual no tiene competencia constitucional, transgrede el principio de reserva de Ley y el principio de especialidad.
- En adición a lo anterior, se sigue que las normas combatidas, transgreden el derecho de protección de los datos personales de todos los ciudadanos, toda vez que si el Constituyente Permanente creó un organismo autónomo especializado en materia de acceso a la información y datos personales, fue para dotar a los ciudadanos de un organismo que fuera garante de esos derechos.

En relación con lo anterior, este Colegio coincide plenamente con los argumentos esgrimidos por el máximo órgano garante de la protección de datos personales en que la emisión del Decreto viola la autonomía constitucional del INAI por las siguientes razones:

- En México, los Órganos Constitucionales Autónomos como el IFT, según se explica más adelante, son instituciones que son creadas mediante mandato constitucional, y es la Constitución la que les otorga su autonomía y facultades para funcionar, por lo que se dice que éstos "actúan con independencia en sus decisiones y estructura orgánica, depositarios de funciones estatales que se busca desmonopolizar, especializar, agilizar, independizar, controlar y/o transparentar ante la sociedad, con la misma igualdad constitucional."[51]
- No obstante, estos órganos también están sujetos al escrutinio del principio de legalidad y como autoridad reguladora deben sujetarse a las disposiciones legalmente y aplicables y solo podrán hacer aquello que la Ley les ordena y autoriza de forma expresa. En este sentido, se debe tener claro que, si bien, la Jurisprudencia de ese Máximo Tribunal ha sostenido la validez de las facultades regulatorias de un órgano como el IFT, estas están subordinadas de forma permanente al principio de legalidad, y en particular, deben entenderse conforme a lo dispuesto en la Constitución y en los términos que fijen las leyes.[52]
- El objetivo primordial del IFT "es el desarrollo eficiente de la radiodifusión y las telecomunicaciones en México con apego a lo establecido en la Constitución. Para lograrlo, debe regular, promover y supervisar el uso, aprovechamiento y explotación de: el espectro radioeléctrico, el uso de redes y la prestación de servicios de telecomunicaciones. Asimismo, es responsable de garantizar el acceso equitativo a infraestructura y otros insumos esenciales para las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluidos los de banda ancha e internet." [53]
- La CPEUM en su artículo 28 establece que el IFT es un órgano autónomo, con personalidad jurídica y patrimonio propio, que tiene por objeto el desarrollo eficiente de la radiodifusión y las telecomunicaciones, conforme a lo dispuesto en la CPEUM y en los términos que fijen las leyes. Asimismo, el texto constitucional precisa que, IFT será también la autoridad en materia de competencia económica de los sectores de radiodifusión y telecomunicaciones.
- Asimismo, el Estatuto Orgánico y la Ley Federal de Telecomunicaciones y Radiodifusión en sincronía con lo dispuesto por la CPEUM establecen que:
    - El IFT es un órgano público autónomo, independiente en sus decisiones y funcionamiento, con personalidad jurídica y patrimonio propios, que tiene por objeto regular y promover la competencia y el

[51] Valentín Ugalde Calderón, Filiberto, "Órganos Constitucionales autónomos", *Revista del Instituto de la Judicatura Federal*, México, núm. 29, Enero 2010, pp. 253-264.
[52] Tesis: P./J. 48/2015 (10a.), Jurisprudencia, Gaceta del Semanario Judicial de la Federación. Libro 25, Diciembre de 2015, Tomo I , página 34.
[53] Información extraída del sitio web del IFT, consultado el 21 de noviembre de 2013, disponible en *http://www.ift.org.mx/iftweb/informacion-general/*

desarrollo eficiente de las telecomunicaciones y la radiodifusión en el ámbito de las atribuciones que le confieren la Constitución y en los términos que fijan esta LFTR y demás disposiciones legales aplicables (Artículo 7, LFTR)

- Artículo 1. El Instituto Federal de Telecomunicaciones es un órgano público autónomo, independiente en sus decisiones y funcionamiento, con personalidad jurídica y patrimonio propio, que tiene por objeto regular y promover la competencia y el desarrollo eficiente de las telecomunicaciones y la radiodifusión en el ámbito de las atribuciones que le confieren la Constitución Política de los Estados Unidos Mexicanos y en los términos que fijan la LFTR y demás disposiciones aplicables. (Artículo 1, Estatuto Orgánico del IFT).

- En relación con las atribuciones del IFT, de acuerdo con lo ordenado por la CPEUM, la LFTR en su artículo 15 establece que el IFT contará con diversas atribuciones relacionadas con la regulación federal de los servicios de telecomunicaciones y radiodifusión, así como la competencia económica en dichos mercados.
- Sin embargo, del contenido de las citadas facultades bajo ningún supuesto se desprende que el IFT tenga atribución legal para ejercer facultades de supervisión policial, prevención de delitos, investigación ministerial, investigación criminal o similares, pues, las facultades de dicho órgano están enmarcada en lo dispuesto en el artículo 28 constitucional que erige a dicho órgano como el máximo regulador de las materias de telecomunicaciones y radiodifusión, excluyendo en consecuencia cualquier poder o habilitación legal para normas otros aspectos distintos de los establecidos en el texto constitucional como podría ser la administración del PANAUT en los términos establecidos por el Decreto que establece en el artículo 176 la atribución del IFT de administrar el citado Padrón y en el artículo 180 Bis la atribución de emitir las disposiciones secundarias para regular la operación del PANAUT.
- Jurisprudencialmente se ha establecido que las facultades del IFT están subordinadas a la competencia material y constitucional que establece el artículo 28 constitucional al señalar, que los párrafos décimo quinto y décimo sexto del artículo 28 mencionado prevvén tres rubros en los que se puede concretar la competencia material del IFT: a) El desarrollo eficiente de la radiodifusión y las telecomunicaciones; b) La regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de radiodifusión y telecomunicaciones, así como del acceso a infraestructura activa, pasiva y otros insumos esenciales, garantizando lo establecido en los artículos 6o. y

7o. de la Constitución; y, c) En materia de competencia económica de los sectores de radiodifusión y telecomunicaciones.[54]

- En este mismo sentido, la jurisprudencia P./J. 49/2015 (10a.) establece que, el artículo 28, párrafo décimo quinto, constitucional prevé claramente que el mandato, como órgano constitucional autónomo del IFT, "tiene por objeto el desarrollo eficiente de la radiodifusión y las telecomunicaciones" y no así otros servicios o aspectos de la actividad nacional o humana. En consecuencia, la regulación del IFT debe proveer a la realización de dicho fin constitucional de una manera no arbitraria ni caprichosa, lo que deberá analizarse caso por caso, e igualmente, debe reconocerse que si el legislador discrepa con los juicios técnicos del IFT puede superarlos mediante la emisión de una nueva ley:
- De acuerdo con la Jurisprudencia de nuestro máximo tribunal la actuación del IFT y en concreto, la facultad regulatoria de la que le pretendió dotar el legislador con la reforma del 16 de abril de 2021 debe quedar circunscrita al desarrollo eficiente de la radiodifusión y las telecomunicaciones, quedando excluida de forma contundente y expresa, cualquier regulación distinta de aquellas materias externas a las competencias en dichas materias que el texto constitucional le ha reservado.
- En este contexto, resulta lógico sostener que, la competencia del IFT es regular a las telecomunicaciones y la radiodifusión, en los términos de la Ley en la materia, no así administrar cualquier actividad de tipo operativo, lo que implicará involucrar a terceros en el tema, con posibles puntos adicionales de vulnerabilidad en el resguardo de la confidencialidad de la información.
- En consecuencia, dotar al IFT de una facultad de operación de un Padrón Nacional de Usuarios de Telefonía Móvil no resulta acorde con el texto constitucional ya que dicho registro ha sido ideado con un propósito completamente distinto al de regular los servicios de telecomunicaciones y radiodifusión y en consecuencia viola de forma flagrante los derechos humanos de legalidad y certeza jurídica.
- Por lo anterior, no se puede sostener que el IFT deba tener facultades legales distintas de las que se desprenden del artículo 28 constitucional como son aquellas de emitir disposiciones en materia de protección de datos personales, máxime cuando el texto constitucional las reserva de forma específica y concreta al INAI.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucionales las disposiciones del Decreto por ser violatorias de los artículos 6o, Apartado A, fracción VIII, primer y segundo párrafos, 16,

[54] Tesis: P./J. 44/2015 (10a.), Jurisprudencia Gaceta del Semanario Judicial de la Federación, Libro 25, Diciembre de 2015, Tomo I, página 36

segundo párrafo, 28, párrafo quince y fracciones XXIX-O y XXIX-S, del artículo 73 de la CPEUM, en tanto que, contrario a lo establecido en los artículos en cita, faculta al IFT a emitir disposiciones en materia de protección de datos personales, lo que viola estos derechos, invadiendo, además con ello, las facultades constitucionales que tiene el INAI.

7. Séptimo concepto de invalidez

Como séptimo concepto de invalidez el INAI indica los artículos 15, fracción XLII Bis, 180 Ter, 180 Quáter, 180 Quintus, Primero, Cuarto y Quinto Transitorios del Decreto son violatorios del artículo 6o, párrafos segundo y tercero, y 7o, párrafos primero y segundo por violar el derecho de toda persona al 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 (párrafo segundo), lo que a su vez transgrede el derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión (párrafo tercero), violándose asimismo la libertad de expresión y la prohibición de la censura, al establecer la obligación de todos los usuarios de telefonía móvil de registrarse en el PANAUT, *so pena* de cancelación del servicio.

En relación con lo anterior, el INAI sostiene con meridiana claridad las siguientes premisas:

- De la lectura sistemática de los preceptos impugnados, se tiene que obligan a todos los usuarios de telefonía móvil a registrarse en el Padrón multicitado, dando sus datos personales, incluidos los sensibles, so pena de cancelación del servicio de telefonía móvil. De igual forma, quienes todavía no son usuarios de este servicio, estarían obligados a proporcionar tales datos como requisito para poder acceder a él.
- El hecho de cancelar el servicio de telefonía, para quienes es la única opción de conexión a Internet, puede restringir seriamente sus posibilidades de acceder a información pública y, de manera general, a información plural y oportuna que no se ve facilitada por medios diversos, de ahí la importancia del reconocimiento de las tecnologías de la información y la comunicación como derechos humanos y como herramientas indispensables para garantizar el acceso universal de la población a la sociedad de la información y el conocimiento, razón por la que ambos fueron incorporados a la Constitución Federal como mandato para el Estado que, desde la entrada en vigor de la Reforma Constitucional de 2013, debe garantizarlos.

- Los artículos impugnados afectan el acceso a información pública, así como el libre acceso a la información plural y oportuna, a través de la telefonía móvil y, además, en contrapartida al último derecho, se está afectando la libertad de expresión, de donde resulta, que esto genera una censura indirecta, prohibida por el segundo párrafo del artículo 7o constitucional.
- El INAI considera que, tomando en cuenta que la cancelación de la línea telefónica móvil genera una limitación directa en el derecho acceso a tecnologías de la información, las cuales sirven a su vez de medio para conocer información pública, plural y oportuna, los artículos impugnados deben ser declarados inconstitucionales al ser contrarios al parámetro de regularidad constitucional.

En relación con lo anterior, este Colegio coincide plenamente con los argumentos esgrimidos por el máximo órgano garante de la protección de datos personales en que la emisión del Decreto **vulnera el derecho humano de acceso a las TIC** por las siguientes razones:

- En relación con las TIC es absolutamente relevante señalar el gran valor e importancia que estas tienen en la sociedad y en la tutela de los derechos humanos. Este concepto es amplio y adopta diferentes connotaciones según el contexto en que se utilice, sin embargo, una definición neutra sobre ellas es la de la Unión Internacional de Telecomunicaciones (UIT) que indica que "el sector de TIC se refiere a equipos y servicios relacionados con radiodifusión, computación y telecomunicaciones, todos los cuales capturan y despliegan información electrónicamente".[55] Las TIC se definen "como herramientas y procesos para acceder, recuperar, guardar, organizar, manipular, producir, intercambiar y presentar información por medios electrónicos" (Sunkel, 2006, p. 8).
- El surgimiento y la extensión masiva del uso de las TIC a finales de la década de 1990 constituyó un hito en la historia de la humanidad, el cual fue conceptualizado de diferentes maneras: *sociedad red, sociedad de la información* y *sociedad del conocimiento,* entre las más reconocidas.[56] En el año 2005 la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco) se decantó por el término de sociedad de conocimiento debido al vínculo que quiso establecer entre el nuevo entorno digital y los retos que representa para el aprendizaje, el fortalecimiento de los derechos humanos y la necesaria relación con los problemas de

[55] "ICT sector refers to equipment and services related to broadcasting, computing and telecommunications, all of which capture and display information electronically." [Traducción de la autora], UIT, *Report of the International Telecommunication Union on information and communication technologies statistics, http://unstats.un.org/unsd/statcom/doc04/2004-16e.pdf* [Fecha de consulta: 21 de mayo de 2021], p. 2.

[56] El término sociedad de la información fue acuñado a finales de los 60 por Masuda (1981) , quien estableció que en las sociedades modernas y avanzadas la generación y transmisión de la información son los principales elementos generadores de riqueza. En tanto que Sociedad del Conocimiento fue creada por Drucker en los noventa, quien destacó que el conocimiento es el principal factor de riqueza; está noción fue agregada a la de información, constituyendo así la SIC (Crovi, 2008).

sostenibilidad ambiental de la sociedad contemporánea (Mansell y Tremblay, 2015).[57]

- En este contexto, las telecomunicaciones, incluida la telefónía móvil y por ende el internet, han sido reconocidas ampliamente como esenciales para el desarrollo social, cultural, económico, político y de la democracia así como para el ejercicio de diversos derechos fundamentales.
- En relación con lo anterior, la Declaración de Principios de la Cumbre Mundial sobre Sociedad de la Información del 12 de mayo de 2004, reconoce la importancia e inmensas repercusiones de las TIC en casi todos los aspectos de la vida y las consideran un instrumento para la productividad, el crecimiento económico, la generación de empleos, el buen gobierno, el diálogo entre personas y naciones así como para mejorar la calidad de vida.
- **El derecho de acceso a las TIC está íntimamente relacionado con la obligación constitucional de que el estado integre a toda la población a la sociedad de la información y del conocimiento. la constitución prevé que esa integración se realizará a través de una política pública de inclusión digital universal.**
- **En el caso del derecho humano al acceso y uso a las TIC pueden mencionarse diversos derechos a los cuales se puede tener acceso si se garantiza efectivamente el primero como el acceso a la educación de calidad, a la libertad de expresión, a la participación política, o los derechos de reunión y asociación.**
- En relación con lo previsto por el tercer párrafo del artículo sexto constitucional el acceso a las TIC, a los servicios de radiodifusión y telecomunicaciones incluidos el de banda ancha e internet, está previsto en México como un derecho humano. Al respecto, debe destacarse que dicho derecho es además un derecho instrumental concebido como un medio sin el cual no sería posible tener en el mundo contemporáneo un acceso pleno al goce de diversos derechos humanos, como se ha reiterado por instituciones de la Unión Europea.[58]
- La Constitución Federal establece que el Estado mexicano, como parte de sus obligaciones en materia de derechos humanos, debe asegurar y garantizar el acceso y disfrute de las tecnologías de la información y la comunicación para reforzar el derecho al acceso a la información y para fomentar la integración de la población con base en la inclusión universal.[59]
- El derecho al acceso y uso de las TIC, tal y como lo ha señalado la Comisión Nacional de Derechos Humanos, “comprende la libertad de las

[57] http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5094/CI_72.pdf?sequence=1&isAllowed=y
[58] Para más información y argumentación sobre este tema, consultar Clara Luz Álvarez, *Internet y Derechos Fundamentales*, Porrúa y Universidad Panamericana, México, 2011.
[59] Álvarez, Clara Luz, *Derecho de los Usuarios de Telecomunicaciones*, Instituto de Investigaciones Jurídicas de la UNAM, México, 2015., http://claraluzalvarez.org/wp-content/uploads/2015/11/Clara-Luz-Alvarez-Dchos-Usuarios-Telecom-2015.pd

personas de acceder y usar eficazmente las tecnologías, navegar por la banda ancha, adquirir información de calidad por los diversos medios digitales, radio y televisivos, difundir cualquier contenido por los medios mencionados, interactuar y formar parte integral de la Sociedad de la Información, sin importar condiciones sociales o económicas."[60]

- Además, la Constitución señala que el Estado mexicano, como parte de sus obligaciones en materia de derechos humanos, debe asegurar y garantizar el acceso y disfrute de las TIC para reforzar el derecho al acceso a la información y para fomentar la integración de la población con base en la inclusión universal.[61] Asimismo, derivado de lo previsto en el artículo sexto, párrafo tercero de la Constitución, el acceso a las TIC y los servicios de telecomunicaciones como es el caso de la telefonía móvil, debe ser libre y sin injerencias arbitrarias.
- De esta suerte, se puede advertir que las telecomunicaciones han sido reconocidas ampliamente como esenciales para el desarrollo social, cultural, económico, político y de la democracia así como para el ejercicio de diversos derechos fundamentales teniendo inmensas repercusiones en casi todos los aspectos de la vida siendo un instrumento para la productividad, el crecimiento económico, la generación de empleos, el buen gobierno, el diálogo entre personas y naciones así como para mejorar la calidad de vida.
- La presencia de las TIC es absolutamente relevante para la garantía de los derechos fundamentales, pues, mediante el acceso a éstas una persona obtiene información para ejercer sus derechos fundamentales, las comunidades se integran socialmente, se puede fortalecer la cohesión social y sin duda también constituyen un insumo básico para la actividad y el desarrollo económico.[62]
- En contraposición, la falta de acceso a las telecomunicaciones en términos equitativos no sólo es un obstáculo para el desarrollo sino también representa un factor para incrementar las diferencias sociales, educativas y económicas.
- El Decreto viola el principio de progresividad de los derechos humanos que se constituye como una obligación del Estado Mexicano de "no adoptar medidas que sin plena justificación constitucional disminuyan el nivel de la protección a los derechos humanos de quienes se someten al orden jurídico del Estado mexicano. Lo anterior, de acuerdo con la Jurisprudencia de nuestro Máximo Tribunal en particular, la tesis de Jurisprudencia 2a./J. 35/2019 (10a.).

[60] http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/foll_DerAccesoUsoTIC.pdf
[61] Álvarez, Clara Luz, *Derecho de los Usuarios de Telecomunicaciones*, Instituto de Investigaciones Jurídicas de la UNAM, México, 2015., http://claraluzalvarez.org/wp-content/uploads/2015/11/Clara-Luz-Alvarez-Dchos-Usuarios-Telecom-2015.pd
[62] https://publications.iadb.org/publications/spanish/document/Diagnóstico-del-sector-TIC-en-México-Conectividad-e-inclusión-social-para-la-mejora-de-la-productividad-y-el-crecimiento-económico.pdf

- Los artículos 180 Bis, 180 Ter, 180 Quater, 180 Septimus último párrafo, 190, fracción VII, Cuarto y Quinto transitorio del Decreto transgreden los siguientes derechos humanos previstos en la CPEUM:
    - El derecho humano al acceso a las tecnologías de la información y comunicación, así como a los servicios de telecomunicaciones, incluido el de banda ancha e internet previsto en el artículo 6º, tercer párrafo y apartado B, fracción VI de la CPEUM.
    - El derecho humano de acceso a las telecomunicaciones en condiciones de cobertura universal, continuidad, acceso libre y sin injerencias arbitrarias previsto en el artículo 6º, apartado B, fracción II de la CPEUM.
    - El derecho a la integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal previsto en el artículo 6º, apartado B, fracción I de la CPEUM.
    - El derecho humano al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión previsto en el artículo 6o, segundo párrafo de la Constitución.
    - El derecho a la libertad de difundir opiniones, información e ideas a través de cualquier medio previsto en el artículo 7º de la CPEUM.
- En consecuencia, la medida prevista en el último párrafo del artículo cuarto transitorio del Decreto que establece que una vez transcurrido el plazo para el registro de titulares o propietarios de las líneas telefónicas móviles, **el IFT solicitará a los concesionarios de telecomunicaciones y, en su caso, a los autorizados, la cancelación en forma inmediata de aquellas líneas de telefonía móvil, que no hayan sido identificadas o registradas por los usuarios o clientes,** constituye una vulneración al derecho de acceso a las TIC en sus distintas manifestaciones ya que impediría a las personas acceder a los servicios de telecomunicaciones e internet en los términos precisados por la Constitución y la normatividad que de ella se desarrolla.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucionales las disposiciones del Decreto por ser violatorias del derecho de toda persona al 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.

8. Octavo concepto de invalidez

Como octavo concepto de invalidez el INAI indica que los artículos 15, fracción XLII Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), Primero, Cuarto y Quinto Transitorios del Decreto son violatorios de la garantía de no retroactividad de la ley en perjuicio de persona alguna, puesto que obra sobre una situación nacida con anterioridad a la norma, respecto de los usuarios que ya cuentan con el servicio de telefonía móvil.

En relación con lo anterior, el INAI sostiene lo siguiente:

- A partir de la reforma a la LFTR, específicamente derivado del artículo cuarto transitorio, para poder conservar tal derecho será necesario registrarse en el Padrón, dando una serie de datos personales. Esto es, la reforma obra sobre una situación actualizada en el pasado, empero, ahora la condiciona al registro, so pena de que el servicio sea cancelado. La norma está obrando hacia el pasado sobre el derecho adquirido de acceder a la información a través de tecnología de información como el servicio de telefonía móvil e internet.
- Pecisamente dicha aplicación retroactiva traerá como consecuencia la afectación de los derechos de acceso a la información pública, de libre acceso a la información plural y oportuna, a través de la telefonía móvil, y de la libertad de expresión, al tenor de lo expuesto en el concepto de invalidez anterior.
- El INAI considera que el artículo cuarto transitorio de la LFTR, es contrario al artículo 14 de la CPEUM, pues crea una norma retroactiva en perjuicio de los particulares que hayan adquirido su línea telefónica con anterioridad a la reforma, por lo que, al actualizar una violación directa a la CPEUM, debe ser declarada inconstitucional.

En relación con lo anterior, este Colegio coincide plenamente con los argumentos esgrimidos por el máximo órgano garante de la protección de datos personales en que la emisión del Decreto **vulnera la garantía de no retroactividad** por las siguientes razones:

- La Segunda Sala de ese H. Tribunal al analizar el concepto de retroactividad de la Ley ha precisado que “el análisis sobre la aplicación retroactiva de una ley implica verificar si el acto concreto se lleva a cabo dentro de su ámbito temporal de validez sin afectar situaciones jurídicas definidas o derechos adquiridos por el gobernado con anterioridad a su entrada en vigor.”[63]
- La Segunda Sala de ese H. Tribunal al analizar el concepto de retroactividad de la Ley ha precisado también que “el análisis sobre la aplicación retroactiva de una ley supone la verificación de que los actos

[63] Registro digital: 181024, Tesis de Jurisprudencia: 2a./J. 87/2004, Semanario Judicial de la Federación y su Gaceta. Tomo XX, Julio de 2004, página 415.

materialmente administrativos o jurisdiccionales estén fundados en normas vigentes, y que en caso de un conflicto de normas en el tiempo se aplique la que genere un mayor beneficio al particular".[64]

- Concretamente, debe recordarse que jurisprudencialmente se ha señalado que "si en un contrato celebrado con anterioridad a la expedición de una ley se crea una situación jurídica concreta, lógico es concluir que sus efectos deben regirse por la ley anterior, por lo que la aplicación de la nueva resultaría notoriamente retroactiva y, la privación de derechos a que da lugar violatoria de la garantía que otorga el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos, en su párrafo primero".[65] Por ello, se entiende que el Contrato de Prestación de Servicios entre concensionarios y usuarios del servicio de telefónía móvil habrá de obedecer esta premisa.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucionales las disposiciones del Decreto por ser violatorias de la garantía de no retroactividad de la ley en perjuicio de persona alguna.

9. Noveno concepto de invalidez

Como noveno concepto de invalidez el INAI indica que los artículos 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), 180 Sextus, así como los transitorios Segundo, Tercero, Cuarto y Quinto de la LFTR, son contrarios a los artículos 17 del PIDCP; 11 de la CADH y 12 de la DUDH, al constituir una injerencia arbitraria al derecho a la privacidad.

De acuerdo con lo anterior, el INAI sostiene lo siguiente:

- Tanto el sistema universal como el sistema interamericano, coinciden en que el derecho a la privacidad es fundamental para una sociedad democrática, pues juega un papel importante, por ejemplo, en la libertad de expresión. Sin embargo, como es un derecho tan amplio, dentro de él se desarrollan otros derechos que comparten las mismas obligaciones de garantía y protección. Uno de esos derechos sin duda es la protección a los datos personales.
- De acuerdo con la DUDH y el PIDCP se deben distinguir 3 cuestiones i) un objeto de protección que es precisamente la vida privada en todos sus aspectos; ii) las obligaciones que deben cumplirse para proteger el objeto y, iii) una prohibición expresa que consiste en no realizar injerencias arbitrarias o ilegales.

[64] Registro digital: 162299, Tesis de Jurisprudencia: 1a./J. 78/2010, Semanario Judicial de la Federación y su Gaceta. Tomo XXXIII, Abril de 2011, página 285
[65] Registro digital: 186047, Tesis de Jurisprudencia: 1a./J. 56/2002, Semanario Judicial de la Federación y su Gaceta. Tomo XVI, Septiembre de 2002, página 88.

- En relación con las obligaciones que deben cumplirse para proteger el objeto, no debe considerarse erróneamente que frente a los artículos 12, 17 y 11 arriba citados, únicamente se actualizan obligaciones de carácter negativo; por el contrario, se exige adecuar todo el aparato estatal bajo conductas omisivas y activas, a efecto de brindar una protección efectiva al derecho a la privacidad.
- Para reforzar esta consideración, la Corte Interamericana, al resolver el caso Fontevechia y D´amico vs Argentina59, determinó que el artículo 11.2 de la Convención Americana protege al individuo frente a la posible interferencia arbitraria o abusiva del Estado, pero que eso no significa que el Estado cumple sus obligaciones convencionales con el solo hecho de abstenerse de realizar tales interferencias, pues el artículo 11.3 de la Convención impone a los Estados el deber de brindar la protección de la ley contra aquellas injerencias. En consecuencia, el Estado tiene la obligación de garantizar el derecho a la vida privada mediante acciones positivas, lo cual puede implicar, en ciertos casos, la adopción de medidas dirigidas a asegurar dicho derecho protegiéndolo de las interferencias de las autoridades públicas así como también de las personas o instituciones privadas, incluyendo los medios de comunicación.
- Finalmente, en lo que respecta injerencias arbitrarias o ilegales, es necesario profundizar en qué es lo que los órganos internacionales han entendido por dicho concepto, pues al establecer que no se permiten las injerencias arbitrarias e ilegales, la interpretación a contrario sensu señalaría que sí puede haber injerencias siempre que no sean de esa naturaleza; por ello, resulta fundamental distinguir cuando se está ante una u otra.
- La creación del Padrón Nacional de Usuarios de Telefonía Móvil, no se ajusta a los parámetros internacionales que integran el parámetro de regularidad constitucional y frente al cual debe analizarse necesariamente la validez del resto de las normas del orden jurídico. Incluso, como apoyo a esta posición, dentro de las consideraciones expuestas por el Alto Comisionado relativas a la creciente práctica de recopilar datos personales para fines de prevención de delitos

En este contexto, el Colegio coincide con el máximo órgano garante de la protección de datos personales por las razones expuestas en el apartado relativo a las violaciones a los derechos de privacidad, vida privada y protección de datos personales, y en particular por las razones que se señalan a continuación:

- **A la vista de los potenciales efectos intrusivos que la creación del PANAUT significa para el derecho de protección de datos personales**, el legislador está obligado a **establecer garantías adecuadas de tipo**

técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental.

- La previsión legal y la legitimidad del fin perseguido son requisitos necesarios pero no suficientes para fundamentar la validez constitucional de una regulación del tratamiento de datos personales, pues para ello se requieren también garantías adecuadas frente al uso potencialmente invasor de la vida privada del ciudadano a través de su tratamiento informático.
- Esas garantías **son necesarias para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos y para que los intereses jurídicamente protegibles, que constituyen la razón de ser del derecho de protección de datos personales, resulten real, concreta y efectivamente protegidos**.
- **La mera inexistencia de «garantías adecuadas» o de las «mínimas exigibles a la Ley» constituye de por sí una injerencia en el derecho fundamental, de gravedad similar a la que causarían intromisiones directas en su contenido nuclear. En el caso concreto, la inexistencia de estas garantías es una afectación directa al derecho de protección de datos personales.**
- La exigencia de «garantías adecuadas» se fundamenta, por tanto, en el respeto del contenido esencial del derecho fundamental a la protección de datos personales, situación que no se actualiza en el caso concreto toda vez que la creación del PANAUT representa una injerencia arbitraria e injustificada al derecho de protección de datos personales, máxime cuando **la necesidad de disponer de garantías adecuadas es especialmente importante cuando el tratamiento afecta a categorías especiales de datos, también llamados datos sensibles, pues el uso de estos últimos es susceptible de comprometer más directamente la dignidad, la libertad y el libre desarrollo de la personalidad**.
- La exigencia de especial protección de esta categoría de datos está prevista en **el Convenio 108**, cuyo artículo 6 establece lo siguiente: «**Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas.** Esa exigencia ha sido igualmente afirmada por la la legislación interna **de acuerdo con … esas garantías adecuadas y específicas para proteger los intereses y derechos fundamentales de los afectados «adquieren una especial relevancia tanto por la**

importancia de los datos personales objeto de tratamiento como por tratarse de tratamientos a gran escala de categorías especiales que entrañarán un alto riesgo para los derechos y libertades de las personas físicas difícilmente mitigable si no se toman medidas adecuadas». (…)

- En conclusión, los datos biométricos **son datos personales sensibles cuya necesidad de protección es, en esa medida, superior a la de otros datos personales. Una protección adecuada y específica frente a su tratamiento constituye, en suma, una exigencia constitucional** el legislador está constitucionalmente obligado a adecuar la protección que dispensa a dichos datos personales, en su caso, imponiendo mayores exigencias a fin de que puedan ser objeto de tratamiento y previendo garantías específicas en su tratamiento, además de las que puedan ser comunes o generales.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconvencionales las disposiciones del Decreto por transgredir el derecho a la privacidad y a la protección de datos personales de los usuarios del servicios de telefonía móvil.

10. Décimo concepto de invalidez

Como décimo concepto de invalidez el señala que los artículos 15, fracción XLII bis, 180 Ter, fracción VI, 180 Quater, 180 Quintus, 180 Séptimus, último párrafo, violan las garantías de seguridad y legalidad jurídicas en relación con las técnicas de investigación contenidas en el artículo 16 constitucional, puesto que permite que acceder a datos biométricos sin control judicial.

De acuerdo con lo anterior, el INAI sostiene lo siguiente:

- Que de acuerdo con lo que ordena el artículo 16 de la Constitución, y toda vez que la toma de datos biométricos constituye en términos del derecho procesal penal una técnica de investigación, que requiere control judicial, se llega a la convicción de que los artículos impugnados transgreden lo establecido por la Constitución Política, al permitir a las autoridades el acceso directo a los mismos, por medio del Padrón.
- Que aun y cuando se hace una remisión a las atribuciones de las autoridades conforme a sus leyes aplicables, lo cierto es que no determina requisitos claros para acceder a la información. Es decir, si será suficiente con que las leyes las autoricen en términos genéricos, o si se requerirá,

además o solamente de su designación en sede administrativa, como lo establece el diverso artículo 18962, segundo párrafo de la LFTR, o si además, o únicamente, se necesitará de una orden judicial para el efecto. El hecho de que se susciten esta serie de cuestionamientos demuestra que la norma en realidad no está cumpliendo con la definición con certeza de los actos que le competen a las autoridades, lo que viola la seguridad jurídica y la legalidad en relación con las técnicas de investigación, toda vez que, la cuestión quedaría en cada caso sujeta a interpretación.

- Que los preceptos en comento y en particular el 180 Séptimus, violan las garantías seguridad y legalidad, toda vez que no establecen con certeza el número de personas que tendrán acceso a datos sensibles como los biométricos, pudiéndose así tener un número indefinido de personas que obtengan tales datos. El artículo en comento no define como será el acceso a los datos biométricos y a los restantes datos personales. Así, pudiera ser posible que se diera acceso a todo el Padrón o que el IFT únicamente diera los datos relativos a una persona. Esto es, no se encuentra definido en qué consistirá ese acceso, lo cual es fundamental de cara a la garantía de legalidad y taxatividad legal. Ya que al tratarse de una intervención en los derechos de protección de datos personales, privacidad, intimidad, identidad y de la niñez, es obligatorio que se haga en respeto al principio reserva de Ley.
- Tampoco se establecen los requisitos que deben contener los requerimientos de acceso a la información del Padrón o acceso al propio Padrón. Esto es, ya que la justificación para introducir la medida legislativa es la persecución de los delitos, entre las exigencias que para su acceso debería contarse, es que la autoridad demostrara que la persona respecto de la cual se solicita la información es sujeto de investigación penal y además, referida al delito de extorsión. Empero, al no ordenarse así, nuevamente será suficiente, en términos de la reforma, que de acuerdo con sus atribuciones los funcionarios tengan facultad expresa para requerir la información, lo cual es violatorio de las garantías en comento, puesto que lo que el legislador debió establecer fue, en su caso, las condiciones de acceso a dicha información y las garantías para su debida protección. Lo contrario es violatorio a los derechos y garantías de seguridad jurídica y legalidad.
- El INAI considera que las reformas incluidas a la LFTR, al no prever la obligación de solicitar autorización previa judicial, se pretende eludir el control judicial, en la obtención de los datos personales, es contrario a los derechos y garantías que reconoce el artículo 16 de la CPEUM.

En este contexto, el Colegio coincide con el máximo órgano garante de la protección de datos personales en que las previsiones del Decreto violan las garantías de seguridad y legalidad jurídicas en relación con las técnicas de investigación contenidas en el artículo 16 constitucional, puesto que permite que acceder a datos biométricos sin control judicial y en particular por las razones que se señalan a continuación:

- La información que formará parte del PANAUT refiere a datos de: i) usuarios de telefonía, ii) titulares de una línea telefónica y iii) usuarios titulares. Lo anterior es contrario al propio contenido del artículo 180 Bis y confuso siendo que el contenido de los artículos del Decreto refieren de forma indistinta a titulares y usuarios omitiendo considerar que puede tratarse de personas diferentes.
- Esta situación genera incertidumbre jurídica puesto que los artículos en comento no definen a quién va dirigida la obligación de proporcionar los datos. La norma jurídica está compuesta en su estructura lógica por el supuesto que refiere a la conducta o estado de cosas regulada, el nexo verbal mediante el que se verifica el supuesto y la sanción que refiere a la consecuencia jurídica prevista.[66] En todos estos elementos mínimos debe estar definido el sujeto normativo. Por tanto, la precisión de quién es el sujeto obligado es un elemento que necesariamente debe estar presente desde la configuración de la norma como uno de sus elementos estructurales.
- Por tanto, el determinar a quién va dirigida una norma no es un elemento susceptible de posterior desarrollo en un Lineamiento o en una reglamentación sino que constituye un elemento estructural a la formulación de la norma que debe ser determinada desde la Ley.
- Por lo anteriormente expuesto los artículos 180 Bis, 180 Ter, 180 Quáter y 180 Quintes así como artículos Cuarto y Quinto transitorios del Decreto carecen de los elementos necesarios para determinar el alcance de las normas que conforman, dejando al gobernado en incertidumbre jurídica en transgresión a los artículos 14 y 16 de la CPEUM en transgresión al derecho de seguridad jurídica y principio de legalidad.
- Los artículos 180 Ter, 180 Quáter, 180 Quintes y el artículo Cuarto transitorio del Decreto transgreden el derecho a la seguridad jurídica y al principio de legalidad contenidos en los artículos 14 y 16 de la Constitución Federal en tanto obligan a dos sujetos a la entrega de datos biométrico: al representante legal de la persona moral titular de la línea telefónica, y al usuario de una línea telefónica. Por otra parte, la

[66] Carla Huerta Ochoa, Conflictos normativos, editado por el Instituto de Investigaciones Jurídicas de la UNAM, IMPRESO EL 3 DE AGOSTO DE 2007, Estado de México, página 21

LFTR deja en total indefinición cuáles son los datos biométricos que se van a recabar.

- Respecto de los datos biométricos la LFTR no establece a qué se refiere con datos biométricos, dejando al titular de la línea telefónica en un estado de incertidumbre sobre la obligación que se lo impone. Esta incertidumbre trasciende además para el usuario de la línea telefónica, así como para los representantes legales de las personas morales. Esta situación se repite en la fracción VI del artículo 180 Ter de la LFTR que también se refiere a los "datos biométricos" del usuario, sin especificar cuáles son serán los que se deben proporcionar como condición para recibir el servicio de telefonía móvil.
- De esta forma, en los términos que está redactado el artículo 180 Ter se podrían requerir desde huellas digitales, iris, rostro, retina, voz, piel, el ADN, etcétera, sin que la LFTR establezca limitación alguna, o bien, justificación sobre las razones porque las que se solicitan dichos datos de naturaleza sensible, lo que deja en estado de incertidumbre jurídica al titular y usuario de las líneas de telefonía móvil, e incluso a los representantes legales de las personas morales.
- En este sentido, para cumplir con los principios de seguridad jurídica y de legalidad, era necesario que el alcance de esta obligación quedara definida desde el texto legal, aportando además los elementos que permitieran justificar que dichos datos debían ser recabados. Más aun, cuando de acuerdo con el artículo 180 Bis de la LFTR el único fin del PANAUT "es el de colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos en los términos de las disposiciones jurídicas aplicables." Por lo que los datos biométricos que sirven para dicha finalidad en todo caso debieron ser definidos por los legisladores.
- El artículo 180 Séptimus del Decreto señala que las autoridades de seguridad de procuración y administración de justicia podrán acceder a la información del PANAUT.
- El referido artículo señala de manera genérica y en violación a los principios de seguridad jurídica y de legalidad, quiénes podrán acceder a la información del PANAUT y cómo podrán acceder a ella. No obstante la relevancia de ambos temas, el legislador no definió quiénes serán las autoridades que podrán acceder a la información. Si bien el artículo dispone que podrán acceder a los datos del PANAUT las autoridades "de seguridad de procuración y administración de justicia" que tengan dentro de sus atribuciones la facultad expresa para requerir al IFT los datos del PANAUT, no las limita en ningún sentido. Esto debido a que no se establece un nivel jerárquico para que solo algunas autoridades

de procuración de justicia accedan a esta información, ni se establece alguna otra limitación que acote a las autoridades.

- Esta situación genera incertidumbre en los usuarios de telefonía y titulares de una línea telefónica debido a que se les está obligando a proporcionar información sin conocer quién tendrá acceso a ella, lo que contraviene los derechos de protección de datos personales y a la autodeterminación informativa.
- Aunado a lo anterior, desde la propia ley no se establecen contrapesos a las facultades de las autoridades que permitan garantizar los derechos de los usuarios y titulares de una línea. Eso así ya que aun cuando los datos del PANAUT son datos sensibles no se establece la obligación de las autoridades de contar con autorización judicial de forma previa al acceso a los datos del PANAUT.
- Se pretende delegar en disposiciones administrativas emitidas por el IFT las normas que regulen el tratamiento de los datos personales y biométricos que se encontrarán en el PANAUT. Lo anterior genera incertidumbre jurídica y contraviene el principio de legalidad en tanto que el IFT no es la autoridad competente para determinar la regulación aplicable al tratamiento de datos personales.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucionales las disposiciones del Decreto por es violar los derechos y garantías que reconoce el artículo 16 de la CPEUM.

11. Décimo primer concepto de invalidez

Como décimo concepto de invalidez el señala que el párrafo segundo del artículo 180 Bis de la LFTR, transgrede el principio de presunción de inocencia, previsto en el artículo 20, apartado B, fracción I, de la CPEUM.

De acuerdo con lo anterior, el INAI sostiene lo siguiente:

- El Decreto precisa de manera textual en su artículo 180 Bis, que el registro del número de una línea telefónica móvil en el PANAUT 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 CPEUM y las demás disposiciones jurídicas aplicables.

- Se indica que la existencia de una línea de telefonía móvil registrada en el PANAUT I, produce la presunción sobre la existencia de la línea, la propiedad y/o titularidad de la misma y la validez de los actos jurídicos relacionados con el contrato de prestación de servicios respectivo. Se trata, según el numeral que se comenta, de una presunción iuris tantum, que admite prueba en contrario. Así, es la consideración de este Instituto accionante, que lo dispuesto por el segundo párrafo del artículo 180 Bis referido, transgrede el principio de presunción de inocencia, reconocido por el artículo 20, apartado B, fracción I de la CPEUM.
- La disposición cuya inconstitucionalidad se reprocha, modifica sustancialmente las premisas en las que se sustenta el principio de presunción de inocencia. Es así, porque supone tres supuestos que concatenados, arriban a una conclusión indubitable en términos de la estructura lógica de la reforma, que no es otra cosa, que la responsabilidad penal por la comisión de un delito.
- El segundo párrafo del artículo 180 Bis de la LFTR, hace precisamente lo contario a lo que postula el principio de presunción de inocencia. Lo hace así, a partir de presumir la titularidad y/o propiedad de una línea de telefonía móvil, en tanto que en el supuesto hipotético que dicha línea se encuentre involucrada en la comisión de un ilícito, su consecuencia inmediata será arrojar la carga de la prueba al titular de la línea y no al acusador.
- La categoría con que será tratado el titular de una línea de telefonía móvil, como consecuencia de esta disposición normativa, será aquella de autor o partícipe en el hecho ilícito. Por otro lado, la disposición que se comenta resulta inconstitucional, en tanto que de hecho da tratamiento de culpable al imputado con lo cual se estaría ante una anticipación de la pena, transgrediendo el principio de trato procesal de la presunción de inocencia.
- La inconstitucionalidad que se reclama, debe ser analizada a partir del esquema de la propia LFTR. Es así, en tanto que la presunción sobre la existencia, titularidad y validez jurídica de la línea de telefonía móvil, tiene coherencia solo en la medida en que la finalidad del padrón, tal y como lo expone el propio numeral, es colaborar con las autoridades de seguridad y justicia. Así, la presunción solo es válida y será efectiva, al momento en que se vincule una línea telefónica con un hecho delictivo. Es entonces, que deviene en inconstitucional, porque atenta precisamente en contra de los postulados esenciales de la presunción de inocencia y carga probatoria. Esto, aún y cuando el mismo numeral disponga que la presunción es conforme a los previsto por el artículo 20 constitucional. Es decir, esa simple referencia no dota de constitucionalidad a la presunción en cuestión, máxime que su esencia es considerar como culpable al titular de una línea de telefonía móvil relacionada con un hecho delictivo.

En este contexto, el Colegio coincide con el máximo órgano garante de la protección de datos personales en que las previsiones del Decreto violan el derecho a la presunción de inocencia por las razones que se señalan a continuación:

- La primera vertiente del derecho a la presunción de inocencia, se puede entender como la obligación de no equiparar a una persona imputada por un delito como responsable por la comisión del mismo y ordena a los jueces a impedir, en la mayor medida de lo posible, la aplicación de medidas que impliquen una equiparación de hecho entre el imputado y el culpable.
- Si bien, el derecho a la presunción de inocencia en el proceso penal prohíbe a los juzgadores equiparar a un imputado con alguien responsable por la comisión de un delito, su aplicación también resulta aplicable a momentos anteriores al proceso penal, o extraprocesales.
- El Decreto establece un sistema complejo a través del cual los titulares de una línea telefónica ahora se encuentran obligados a registrar información en el PANAUT, no solo información propia, sino también del usuario de la línea en los casos en que éste sea distinto, información que será utilizada como una presunción en materia de procuración de justicia.
- El artículo 180 Bis, segundo párrafo de la LFTR señala que a partir de la información que se haga constar en el Padrón, se actualizan las siguientes presunciones:
    a. La existencia de la línea telefónica registrada.
    b. Que la línea telefónica pertenece a la persona que aparece en el PANAUT como titular o propietaria.
    c. Los datos que se encuentran registrados en el PANAUT en términos del artículo 180 Ter.
    d. Que los actos jurídicos que se relacionan con la línea telefónica fueron realizados por su titular, o incluso, por su usuario.
- El hecho de que el artículo 180 Bis se refiera a “actos jurídicos” no otorga garantía alguna a los particulares, sino, los deja en un mayor estado de indefensión, ya que en términos de la legislación no se cuenta con una definición precisa de los actos jurídicos.
- El hecho de que las disposiciones del Decreto incluyan diversas categorías de sujetos que deberán entregar sus datos para conformar el PANAUT y que las normatividades de carácter similar recomiendan separar, tales como los sospechosos, los condenados por una infracción penal, las víctimas o los terceros, entre los que se incluyen los testigos, las personas que posean información o contactos útiles y los cómplices de sospechosos y delincuentes condenados, es suficiente para determinar que el Decreto es

contrario al derecho de presunción de inocencia y protección de datos personales.

- La presunción de atribuir determinados actos al titular de la línea, modifica las premisas en las que se basa el principio de presunción de inocencia en tanto que, sin necesidad de probanza alguna se tiene al titular de la línea como responsable de las actuaciones efectuadas a través de ella, pero incluso, en los casos en los que el titular de la línea sea distinto al usuario, se deja a la discrecionalidad de la autoridad atribuir dichas presunciones.
- La situación que se plantea en el párrafo anterior hace evidente la inconstitucionalidad no solo del artículo 180 Bis de la LFTR que establece las presunciones relacionadas con los datos del PADRÓN para su uso en materia de seguridad y justicia, sino también la inconstitucionalidad del sistema en su conjunto en tanto establece:
    a. La obligación de proveer datos del titular y del usuario de la línea de telefonía móvil.
    b. Sujetar el acceso a las tecnologías de la información y comunicación, a la condición de entregar datos personales que serán utilizados para la persecución de delitos.
    c. La cancelación de los servicios de telecomunicaciones a través de un teléfono celular, en el caso de que no se realice el registro en el PADRÓN, así como la imposibilidad para obtener una nueva línea de telefonía móvil.
- La presunción que se establece en el Decreto resulta inconstitucional en tanto le atribuye a la información que obre en el Padrón la calidad de prueba, esto es, se le reconoce como un medio de prueba que podrá ser utilizado por las autoridades en materia de seguridad y justicia para la persecución de delitos.
- A la presunción que atribuye al titular los hechos vinculados con la línea se suma la consecuencia de la suspensión de la línea, todo esto sin que exista un estándar que determine el nexo causal entre el titular de una línea telefónica y la comisión o relación con un hecho delictivo más allá de la simple presunción contenida en el artículo 180 Bis de la LFTR.
- La presunción contenida en el artículo 180 Bis de la LFTR modifica las reglas probatorias al atribuir al titular de la línea los hechos relacionados con ella, y revertir al titular la carga de la prueba.
- El Decreto establece en su artículo Sexto transitorio la obligación de los concesionarios y autorizados de telefonía a incentivar la obligación de sus clientes o usuarios de “denunciar en forma inmediata el robo o extravío de sus equipos celulares o de las tarjetas de SIM, así como para prevenir el robo de identidad y el uso ilícito de las líneas telefónicas móviles, así como en los casos que se trate de venta o cesión de una línea telefónica móvil.”

Con esto, se pretende trasladar al propio usuario o cliente de telefonía la carga probatoria de acreditar su inocencia mediante la denuncia del robo o extravío de un teléfono celular a fin de pretender desvirtuar la atribución de las conductas relacionadas con la línea.

- Adicionalmente como resultado de la presunción contenida en el artículo 180 Bis se generan externalidades negativas como lo son incentivar el robo de identidad y de teléfonos móviles. Dicha presunción también podría generar consecuencias en contra la falta de denuncia del robo de un teléfono móvil. Situación que no es menor, en tanto que de acuerdo con la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) de 2020, realizada por el INEGI, se estimó que en nuestro país existe un cifra negra de 92.4% de delitos que no se denuncian o no se inicia una carpeta de investigación, por lo que sostener una presunción en contra de quien no denuncie trastoca los derechos de los usuarios de telefonía móvil así como también los principios del sistema acusatorio penal y de seguridad jurídica.
- Esta situación revictimiza a quien sufra el robo de un teléfono móvil o la suplantación de identidad.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucional el artículo 180 bis de la LFTR por ser contrario al principio de presunción de inocencia, previsto en la fracción I, del inciso B, del artículo 20 de la CPEUM.

12. Solicitud de suspensión

En la demanda de acción de inconstitucionalidad el INAI solicitó a ese H. Tribunal la suspensión de los efectos y consecuencias de las reformas publicadas a la LFTR, a efecto de paralizar los daños pueden causar las obligaciones de registro derivadas de tal normativa por considerar que no existe impedimento jurídico para dictar una medida suspensional en sentido favorable, aunado a que con este pronunciamiento no se pone en peligro la seguridad o el orden público, las instituciones fundamentales del orden jurídico mexicano, ni se afecta gravemente a la sociedad sino que, por el contrario, de no concederse la medida solicitada se afectarían irreparablemente los derechos fundamentales que se aducen como vulnerados a lo largo de esta demanda, ocasionando con ello daños irreversibles a los titulares de líneas de telefonía móvil.

Respecto de este particular y toda vez que ese H. Tribunal ha decretado la negativa a la suspensión solicitada por el INAI, este Colegio, considera importante precisar que de acuerdo con el artículo 1 de la CPEUM y 64 de la Ley

Reglamentaria de las fracciones I y II de la Constitución Política de los Estados Unidos resulta factible conceder la suspensión respecto de normas generales en la acción de inconstitucionalidad “en aquellos casos en que la controversia se hubiera planteado respecto de normas generales que impliquen o puedan implicar la transgresión irreversible de algún derecho humano”, máxime que, como se ha señalado en el presente documento de no suspenderse la aplicación del Decreto se estarían actualizando las violaciones a diversos derechos humanos entre ellos la privacidad, vida privada, protección de datos personales, dignidad, libertad de expresión, presunción de inocencia, acceso a las TIC, legalidad, seguridad jurídica, entre otros.

VII. Argumentos relacionados con los conceptos de invalidez hechos valer por Senadores de la República, integrantes de la LXIV Legislatura

En la acción de inconstitucionalidad 86/2021 los Senadores integrantes de la LXIV Legislatura reclaman como norma impugnada el Decreto estimando violados los artículos 1o, 14, 16, 72, 74 y 134 de la CPEUM y como conceptos de invalidez los siguientes.

1. Primer concepto de invalidez

Como primer concepto de invalidez, los Senadores integrantes de la LXIV Legislatura sostienen que, para la emisión del Decreto consideran que tanto en la Cámara de Diputados como en la de Senadores no se fundamentaron y motivaron de forma correcta los dictámenes correspondientes. Esto se argumenta de la forma siguiente:

- *Indebida Fundamentación del Dictamen Legislativo en la Cámara de Diputados.*
    - Su fundamentación inicial en los artículos 189 y 190 de la Ley Federal de Telecomunicaciones es insuficiente, toda vez que “la obligacion de colaborar no implica asumir un costo económico para obtener el equipo necesario para recabar datos biometricos, ni realizar actos que serian propios de autoridades”. Por otra parte, se confunde las autoridades del artículo 6 de CPEUM. Esto se basa en la cita de la Cámara del artículo 1 del la LGPDPPSO y se alude a que la competencia de proteger los datos personales recae en el IFT y no en el INAI.
    - Esto genera una contravención al artículo 6 de la CPEUM, pues establece un régimen diferenciado para ambos institutos.
    - Al justificar la idoneidad de la medida con un estudio realizado por la misma Cámara, no se aluden a los principios del gasto público del artículo 134 de la CPEUM, pues, aunque se establezca que no se

existe carga presupuestal al existir capacidad y estructura, existe la carga presupuestaria al aumentar el volumen de trabajo para el IFT.

- Finalmente se alude a la posible violación al principio de presunción de inocencia, pero no se resuelve al momento de emitir la norma aprobada.

- *Indebida motivación del Dictamen Legislativo en la Cámara de Diputados*
  - Su fundamentación no profundiza lo suficiente, pues se tratan de derechos humanos "tocados por la reglamentación de datos personales sensibles".
  - En la exposición del primer considerando, no se toma en cuenta el manejo de datos personales y, cuando se hace, se realiza de forma sesgada.
  - La dictaminadora hizo caso omiso a las recomendaciones de expertos en donde se plantea la necesidad de un trabajo mayor en materia de datos personales y presunción de inocencia.
  - Dentro de la misma dictaminación, se señalan otros mecanismos, en donde no habría necesidad de crear un Padrón tan invasivo y se debió haber ponderado la protección de datos sensibles con la seguridad pública. Sobretodo, considerando que se trata de una afectación estimada a más de 80 millones de personas y se necesita un análisis reforzado al respecto.
- *Indebida fundamentación y motivación del Dictamen Legislativo en la Cámara de Senadores*
  - Principalmente, se enfoca en justificar la necesidad de la reforma, pero omite ofrecer sustento en normativa adicional.
  - El dictamen contempla el combate al delito por medio de la sanción, considerando así el registro de identidad, en vez de buscar implementar medidas preventivas o complementarias.
- *Violaciones a las formalidades esenciales del Proceso Legislativo en la Cámara de Senadores*
  - De acuerdo con los Senadores estas consisten en: La participación de todas las fuerzas políticas en condiciones de igualdad; La aplicación correcta de las reglas y la publicidad del debate y las votaciones.

En este contexto, el Colegio apoya los argumentos de los Senadores integrantes de la LXIV Legislatura y considera fundamental su análisis desde el tamiz de la proporcionalidad de la medida a partir de lo siguiente:

- El fin de persecución del delito ya dispone de diversas herramientas legales. Muy en concreto, respecto de la colaboración con las autoridades

de los concesionarios y autorizados de servicios de telecomunicaciones se encuentran ya diversos mecanismos:

- Los artículos 252, 252, 291, 301 y 303 del Código Nacional de Procedimientos Penales.
- El artículo 34 de la Ley de Seguridad Nacional.
- La Ley de la Guardia Nacional .
- La fracción I del artículo 190 de la LFTR
- La fracción II del artículo 190 de la LFTR

- La medida contraviene lo establecido en los artículos 1, 6, 16, 29 de la CPEUM, entre otros, pues de forma clara esta medida incide de forma negativa en los derechos de vida privada, privacidad, protección de datos personales y representa una restricción injustificada, arbitraria e ilícita al derecho de protección de datos personales, entre otros.
- La medida no resulta adecuada o racional porque no constituye una medida adecuada para alcanzar el fin perseguido, toda vez que, de un lado, el legislador ni siquiera realizó la previa ponderación de los intereses en pugna. Esto es, omitió definir todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas, y, de otro, porque, de haberlo realizado, habría llegado a la conclusión de que la medida era inadecuada porque todos los resultados empíricos demuestran que la creación de un registro de esta naturaleza no tiene como consecuencia lógica la disminución en los índices delictivos, en particular, respecto de delitos cometidos mediante el uso de dispositivos móviles de comunicación a través de redes de telecomunicaciones, esto es, no existe evidencia de que este tipo de registros influya en la reducción del delito:
  a. El Padrón Nacional de Usuarios de Telefonía Móvil es, en términos generales, una reedición del fallido Registro Nacional de Usuarios de Telecomunicaciones (RENAUT),
  b. El RENAUT fue eliminado en 2011 debido a que su base de datos fue filtrada y puesta a disposición en el mercado negro. En vez de incidir en la reducción de la delincuencia, los delitos de extorsión y secuestro repuntaron en 40 y 8 por ciento, respectivamente, durante el periodo de vigencia del registro.[67]
  c. En junio de 2012 la Secretaría de Gobernación eliminó la base de datos del Registro Nacional de Usuarios de Telefonía Móvil (RENAUT) que almacenaba 98 millones 455 mil 246 números telefónicos y la Clave Única del Registro de Población de su propietario. A través de un script computacional se destruyó la información contenida en las llamadas

[67] https://www.infobae.com/america/mexico/2021/04/14/por-que-el-padron-de-celulares-fue-comparado-con-el-renaut-y-que-riesgos-hay/

tablas de verificación en la que aparecían los números telefónicos y la CURP. [68]

d. A la fecha, solamente 17 países en el mundo exigen algún tipo de identificación biométrica como China, Arabia Saudita, Afganistán, Venezuela, Emiratos Árabes Unidos, Tayikistán.[69]

e. Un número creciente de gobiernos ha implementado recientemente el registro obligatorio de usuarios de tarjetas SIM prepagas, principalmente como una herramienta para la lucha contra el terrorismo y para mejorar la aplicación de las leyes. Sin embargo, hasta la fecha no hay evidencia de que el registro obligatorio conduzca a una reducción del delito. Otra serie de gobiernos, entre ellos el del Reino Unido, la República Checa, Rumania y Nueva Zelanda, han considerado exigir el registro de tarjetas SIM prepagas y decidieron no hacerlo. [70]

f. Canadá, República Checa, Nueva Zelanda, Rumania y el Reino Unido han optado por no materializar su creación. En el Reino Unido, por ejemplo, este tema fue examinado en detalle por un grupo de expertos de representantes de las fuerzas del orden, agencias de seguridad e inteligencia y proveedores de servicios de comunicaciones luego del ataque terrorista en Londres en julio de 2005. Un informe confidencial de expertos concluyó que “el registro obligatorio de propiedad de teléfonos móviles no reportaría nuevos beneficios significativos al proceso de investigación y diluiría la eficacia de los actuales esquemas de autorregistro. Esto es**,** la medida tendría que haber sido precedida de un análisis real y práctico, teniendo en cuenta datos estadísticos y los resultados de la investigación internacional existentes, para demostrar que es necesaria. Reiteramos, de haber realizado esta ponderación, la medida no habría superado el parámetro de necesidad para la restricción de derechos.

g. El 18 de febrero de 2020, el Tribunal Constitucional rumano declaró por unanimidad inconstitucional un nuevo acto legislativo adoptado en septiembre de 2019 que introduce el registro obligatorio de la tarjeta SIM. El acto legislativo en cuestión era una ordenanza de emergencia emitida por el Gobierno que quería introducir esta obligación como una medida “para mejorar el funcionamiento del número 112 del servicio de emergencia”. Esta es la segunda vez que el tribunal emite una decisión de inconstitucionalidad sobre las propuestas de registro de tarjetas SIM obligatorias. [71]

[68] https://www.animalpolitico.com/2012/06/segob-elimina-base-de-datos-del-renaut/
[69] https://www.eluniversal.com.mx/cartera/telecom/advierten-que-nuevo-registro-de-telefonia-movil-no-detendra-extorsion-y-secuestro
[70] https://www.gsma.com/latinamerica/wp-content/uploads/2014/06/GSMA_White-Paper_Registro-UsuariosPrepagos.pdf
[71] https://edri.org/our-work/romania-mandatory-sim-registration-declared-unconstitutional-again/

h. En Alemania, el Tribunal Administrativo de Wiesbaden consideró desproporcionado el registro general del uso del teléfono, el teléfono móvil, el correo electrónico e Internet de toda la población (conocido como retención de datos). En su decisión el tribunal precisó lo siguiente: "*la conservación de datos viola el derecho fundamental a la privacidad. No es necesario en una sociedad democrática. El individuo no provoca la interferencia pero puede ser intimidado por los riesgos de abuso y la sensación de estar bajo vigilancia [...]*[72]

i. En la Unión Europea, algunos Estados Miembros adoptaron medidas solicitando el registro de tarjetas SIM, y en 2012 la Comisión Europea (CE) invitó a todos los Estados Miembro a presentar pruebas del beneficio real o potencial de tales medidas. Tras examinar las respuestas, Cecilia Malmström, Comisaria Europea de Asuntos Interiores, señaló que: *"Actualmente no hay evidencia, desde el punto de vista de las ventajas para la investigación judicial o el buen funcionamiento del mercado interno, de la necesidad de un enfoque común del la UE en este ámbito."* [73]

j. En 2011 Colombia creó su registro del IMEI (identificador único) operado por las firmas de telefonía móvil y el regulador telecomunicaciones en ese país, sin embargo, desde su instrumentación hace una década, las cifras oficiales indican que el hurto de dispositivos móviles se disparó y anualmente se denuncia un millón de hurtos de celulares. [74]

k. La creación del Padrón no contribuye a reducir los niveles de inseguridad. "Ningún delincuente usará una línea previamente registrada a su nombre para cometer un ilícito". El Registro Nacional de Usuarios de Telefonía ("RENAUT" 2009-2012) que representa el antecedente inmediato del Padrón tuvo, entre otros, los siguientes problemas: no coadyuvó al abatimiento del secuestro y de la extorsión; incentivó el robo de datos personales; los delincuentes utilizaron celulares o SIMs robados o adquiridos en el mercado negro, que seguramente no estaban registrados a nombre del propio delincuente; se produjo la suplantación de los titulares de las líneas celulares.

l. En Colombia, Uruguay, Argentina e incluso en México, la creación de un padrón nacional de usuarios de telefonía celular ha fracasado en su intento por detener el robo, la extorsión y el secuestro, advirtieron expertos. [75]

[72] http://www.vorratsdatenspeicherung.de/content/view/301/79/lang,en/
[73] https://www.gsma.com/latinamerica/wp-content/uploads/2014/06/GSMA_White-Paper_Registro-UsuariosPrepagos.pdf
[74] https://www.elfinanciero.com.mx/empresas/2021/04/20/los-padrones-de-telefonos-celulares-han-fracasado-a-nivel-mundial-por-que/
[75] https://www.elfinanciero.com.mx/empresas/2021/04/20/los-padrones-de-telefonos-celulares-han-fracasado-a-nivel-mundial-por-que/

m. En su comunicado de marzo de 2021, la industria de telecomunicaciones afiliada a CANIETI,[76] se opuso a la aprobación de la Iniciativa de reforma a la LFTR, considerando, entre otras, las razones reales y concretas siguientes: 1) No contribuirá a reducir los niveles de inseguridad; existen infinidad de maneras en la que la delincuencia puede establecer comunicaciones sin registro o control. En ningún país del mundo este tipo de registros han probado su efectividad; 2) Contribuirá a la incidencia de delitos; los delincuentes pueden cometer ilícitos con equipos conseguidos por la comisión de aquellos, como sucede por ejemplo con automóviles o motocicletas; 3) Se fomentará más el robo de dispositivos, sobre todo en el caso de prepago. Esto ha quedado demostrado en los reportes de Locatel de la campaña "bloquea tu celular" y 4) No atenderá la necesidad de contrarrestar, entre otras acciones, las llamadas de extorsión que se generan desde números de prepago. La Iniciativa debía indicar que quien efectúa el registro es el usuario de los servicios de telecomunicaciones, en tanto que éstos deberían tener el control y conocimiento del tratamiento que se dará a sus datos personales.

n. El Reporte El Registro Obligatorio de Usuarios de Tarjetas SIM Prepagas de GSMA[77] ha señalado que no hay evidencia empírica para demostrar que: 1) La obligatoriedad del registro de usuarios de SIM prepago conduce a una reducción en la actividad delictiva; y 2) La ausencia de registro de usuarios de tarjetas SIM prepagas esta se vincula con un mayor riesgo de actividades delictivas o terroristas.

o. El Reporte reporte Registro obligatorio de tarjetas SIM prepago de GSMA [78]enfatiza que "el registro de la tarjeta SIM prepago es obligatorio en varios países y requiere que los consumidores proporcionen un comprobante de identificación para activar y usar una tarjeta SIM móvil. Varios gobiernos adoptan esta política como parte de los esfuerzos para ayudar a mitigar los problemas de seguridad y abordar el comportamiento delictivo y antisocial. **Hasta la fecha, no ha habido evidencia empírica de que el registro obligatorio de SIM conduzca directamente a una reducción de la delincuencia.**

- Han sido diversos los mecanismos que de forma sustitutiva a la creación del Padrón se han recomendado e identificado, siendo la creación del aludido Registro una medida altamente cuestionada de forma previa a su instrumentación, en particular, se ha señalado que:

[76] http://www.canieti.org/Libraries/com/INICIATIVA_REGISTRO_DE_USUARIOS.sflb.ashx
[77] https://www.gsma.com/latinamerica/wp-content/uploads/2014/06/GSMA_White-Paper_Registro-UsuariosPrepagos.pdf
[78] GSMA, Mandatory registration of prepaid SIM cards Addressing challenges through best practice, abril de 2016, p.2, disponible en *https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf*

a. Existencia de mecanismos legales habilitadores para estos fines: además de la legislación general y extensa en materia de seguridad y prevención de delitos y de las facultades de las autoridades competentes, muy en particular respecto del acceso a los datos derivados de los servicios de telecomunicaciones:
b. La posibilidad de acceso no suficientemente controlado a estos tratamientos de datos personales arroja ya en la actualidad serias cifras de abusos por parte de la autoridad.
c. En suma, incluso en la situación actual, ha existido un abuso sistemático y generalizado de las facultades de investigación que invaden la privacidad de personas usuarias de telefonía móvil,
d. Por lo tanto, la ausencia de la creación del Padrón que pretende aprobarse no impide a las autoridades combatir delitos como el de extorsión, sino que constituye un pretexto inaceptable para maquillar la incompetencia de las instituciones de seguridad o intenciones autoritarias, además de que es ilegal.
e. No existe en el país registro alguno, público o privado, que pueda contener mayor cantidad de información sensible de los particulares, además de información personal y de localización, hábitos de consumo, y demás datos personales. **El derecho a la privacidad es uno de los pilares de las sociedades democráticas y, como tal, desempeña un papel importante para la realización de los derechos a la libertad de expresión y a opinar sin injerencias. así como a las libertades de reunión y asociación pacíficas.** Asimismo, debido a la interconexión de una variedad de derechos humanos, los impactos adversos pueden apuntar aún más lejos y comprometer un amplio espectro de derechos. Estos incluyen, entre otros, **el derecho a la igualdad de protección ante la ley, derecho a la no discriminación, los derechos a la vida, a la libertad y seguridad de la persona, un juicio justo y debido proceso, el derecho a la libertad de movimiento, el derecho a disfrutar del más alto nivel posible de salud, y tener acceso al trabajo**. Estas preocupaciones están particularmente bien fundamentadas cuando se exploran cuestiones relacionadas con los datos biométricos y las herramientas impulsadas por dichos datos.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucional el Decreto por virtud de que la ausencia de debida fundamentación y motivación legal del mismo.

2. Segundo concepto de invalidez

Como segundo concepto de invalidez, los Senadores integrantes de la LXIV Legislatura sostienen que, adicionalmente a la ausencia de fundamentación y motivación en los dictámenes parlamentarios, y a la falta de seguimiento de las formalidades esenciales del procedimiento legislativo, existe también una falta al principio de legalidad por la forma en que está diseñada la normativa que se impugna.

De acuerdo con lo anterior, los Senadores integrantes de la LXIV Legislatura sostienen lo siguiente:

- Se señala que el núcleo de la reforma a la LFTR se encuentra en la interrelación de los artículos 180 Bis, donde se crea el PANAUT y establece su finalidad; 180 Ter, que marca la información que debe contener el Padrón; el 180 Quáter, que establece la obligatoriedad del registro en el Padrón para poder activar una línea telefónica móvil y el 180 Quinquies, que obliga a los operadores de telecomunicaciones a recabar los datos del PANAUT.
- Se precisa que son los operadores de telecomunicaciones los que deben recabar los datos biométricos de los ciudadanos que sean usuarios de telefonía móvil, para después transferirlos al IFT, que será el que mantenga el resguardo de los datos. Asimismo, cualquier actualización debe llevarse a cabo inicialmente por los operadores y después registrada por el IFT; invariablemente si se tiene o no una línea registrada, una vez recabados los datos biométricos se mantendrán por seis meses.
- El artículo 16 constitucional establece que nadie puede ser molestado entre otras cosas, en sus posesiones, sin que haya una orden escrita estableciendo la ley aplicable y la justificación para ello. Los datos biométricos, habremos de ver, son un tipo de dato personal que dimana del cuerpo: como lo son el iris, la voz y la huella digital; son partes de nosotros y, por lo tanto, son nuestra propiedad, pues nadie mas los puede generar más que nosotros.
- Al solicitar datos que son propiedad de las personas, la normativa que regula el Padrón debe fundamentar, que en este caso consiste en tener un asidero jurídico sólido y no contravenir la legislación existente en materia de datos personales. Esto no se da, pues existe una contravención directa con la LGDPPSO que establece en su numeral sexto una serie de principios rectores en materia de datos personales. Estos son: *licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad*.
    - De estos, resulta importante mencionar el de calidad, proporcionalidad, lealtad y responsabilidad. El primero, contenido en el artículo 11 de la LGDPPSO, establece que los datos personales sean pertinentes y correctos para los fines para los que fueron

recabados. Esto no se da, toda vez que se piden datos personales sensibles (incluidos aquellos relativos al cuerpo de las personas) para crear instrumentos de apoyo para las autoridades de seguridad pública y de justicia, que en el pasado no han servido.

- Entonces, recabar datos personales sensibles para crear un padrón que en el pasado ha fallado el propósito para el que fue creado y que en la reforma tiene una versión más invasiva y ambigua, pues no especifica los delitos para los que puede ser usado, a diferencia del primer padrón, violenta el principio de calidad.
- El principio de responsabilidad del artículo 14 de la LGDPPSO contempla que "El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación". Consideramos que este principio se violenta cuando se pone una carga a los operadores de telecomunicaciones y al IFETEL que va más allá de su diseño organizacional y que le impone una fuerte obligación económica.
- El principio de proporcionalidad está contenido en el artículo 13 de la Ley y prevé que el tratamiento de datos personales sea el "necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad". En el caso que nos ocupa, la proporcionalidad se debe dar con respecto a las finalidades de la Ley; la norma establece como finalidad la creación de un instrumento para combatir el delito y prevé para cumplirla que la ciudadanía de sus datos personales más sensibles.
- De lo anterior se concluye que las reformas a la LFTR son contrarias al principio de proporcionalidad y constituye una indebida motivación, pues el cambio realizado es desproporcionado a su finalidad. Asimismo, estas violaciones constituyen, como un conjunto, una indebida fundamentación, pues contravienen directamente la LGPDPPSO y constituyen una violación directa al artículo 16 constitucional.

En este contexto, el Colegio apoya los argumentos de los Senadores integrantes de la LXIV Legislatura y considera que, en efecto, el Decreto vulnera los principios de protección de datos personales previstas en la LGPDPPPSO por las siguientes razones: *licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad*

- Los principios, deberes y derechos de protección de datos previstos en la normatividad aplicable configuran al derecho humano a la protección de datos personales como tal, de modo que constituyen su núcleo básico o esencial **y por tanto cualquier fallo o violación de cualquiera de estos principios que**

configuran este derecho humano implica una violación del propio derecho.

- El Decreto resulta inconstitucional toda vez que la creación del PANAUT implica una indubitable transgresión de los principios y deberes de protección de datos previstos en la LFPDPPP y la LGPDPPSO como se expone a continuación:
    - ***Violación al principio de licitud:*** La violación al principio de licitud que configura el derecho a la protección de datos se materializa con la creación del Padrón porque el IFT carece de facultades y atribuciones para instalar, operar, regular y mantener el PANAUT de acuerdo con la finalidad del mismo. Derivado de la propia naturaleza del Padrón ya se advierte la ausencia de habilitación legal al IFT para gestionar dicho registro, pues:
        - El IFT como órgano regulador de los sectores de telecomunicaciones y radiodifusión, no cuenta con ninguna atribución y/o facultad legal que le legitime para el ejercicio de ninguna de las dos funciones señaladas, y
        - La gestión del derecho a la identidad está reservada a la Secretaría de Gobernación, a través del Registro Nacional de Población,[79] como reserva de ley expresa, formal y material, mediante la Ley General de Población cuyo artículo 85 establece que la SEGOB tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero,[80].
        - En definitiva, existe, una ilegitimidad para el IFT de doble vertiente: activa (invasión de la esfera de atribuciones y facultades de la SEGOB) y pasiva (carencia de atribuciones).
        - En virtud de lo anterior, se puede considerar que el hecho de que el legislador federal atribuya al IFT una facultad legal, **contraria a lo establecido por el texto constitucional resulta violatoria de los derechos humanos de legalidad y seguridad jurídica, al constituir una ampliación arbitraria e infundada de las atribuciones constitucionales de dicho órgano regulador con base en lo dispuesto por el artículo 28 de la CPEUM, que además supone una intromisión ilícita en las facultades y competencias de otras autoridades que están legalmente facultadas para las materias que se pretenden atribuir ilícitamente al IFT.**

[79] Artículo 86.- El Registro Nacional de Población tiene como finalidad registrar a cada una de las personas que integran la población del país, con los datos que permitan certificar y acreditar fehacientemente su identidad.
[80] Artículo 85.- La Secretaría de Gobernación tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero.

- ***Violación al principio de finalidad***. El Decreto y la creación del PANAUT violan el principio de finalidad por las siguientes razones:
  - El principio de finalidad regulado tanto en el Convenio 108 como en la LFPDPPP y en la LGPDPPSO establece la obligación de que la obtención y tratamiento de los datos personales deberán sujetarse a finalidades **explícitas, legítimas y determinadas.**
  - En relación con el referido principio, el Convenio 108, en su artículo 5, obliga al Estado Mexicano a establecer medidas para que los datos personales en posesión de sujetos obligados, como lo es el IFT, únicamente sean sujetos a tratamiento cuando **existan fines determinados y legítimos**, prohibiéndose su utilización de forma incompatible con dichos fines. En el presente caso es indudable que el Decreto reclamado vulnera el principio de finalidad y por ende el derecho humano de protección de datos personales en virtud de que:
    - La finalidad explícita por la que se pretende justificar el **Padrón** (colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos cometidos a través de líneas celulares) no resulta adecuada o racional porque no constituye una medida que permita alcanzar el fin perseguido, y es en realidad una finalidad eventual respecto de la **verdadera finalidad** que consiste en la "identificación plena y certera de los titulares de las líneas de comunicación, a través del Padrón" y, solo de forma eventual, en caso de cometerse un delito con la línea celular, emplear esa información para su persecución, por lo que el Padrón tiene un fin primario de registro y control de las personas a través de líneas telefónicas móviles, desde el momento de su adquisición, y
    - El IFT carece de atribuciones o competencias para la realización de este tratamiento, e invade competencias reservadas formal y materialmente por ley.
- ***Violación al principio de proporcionalidad***. Se configura una violación al principio de proporcionalidad previsto en la normatividad vigente en virtud de lo siguiente:
  - El principio de proporcionalidad está previsto en el artículo 5o, inciso c, del Convenio 108, el cual determina que los datos de carácter personal que los Estados recopilen serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado, situación que no se cumple con la

sola creación del PANAUT que ordena recabar datos biométricos sensibles sin que exista una adecuada justificación legal.

- La LGPDPPSO – artículo 25 - y la LFPDPPP – artículo 13-, de forma similar, establecen que **el responsable solo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento,** situación que no se cumple con la sola creación del PANAUT que ordena recabar datos biométricos sensibles sin que exista una adecuada justificación legal.
- El Decreto **vulnera el principio de proporcionalidad** y por ende el derecho humano de protección de datos personales en virtud de que, como se demostrará a continuación:
    - Los datos personales objeto del tratamiento del Padrón **son excesivos** para la finalidad de colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos cometidos a través de líneas celulares, ya que los datos personales objeto del tratamiento del Padrón son de una naturaleza tendiente a crear un registro de identidad que permiten certificar y acreditar fehacientemente la identidad de los ciudadanos, finalidad que no es compatible con la finalidad para la cual fue creado el Padrón.
    - Obliga al tratamiento de **datos personales biométricos**, mismos que constituyen datos personales sensibles sin que exista legitimación alguna que lo permita ni sea proporcional su tratamiento.
    - Existe una **conservación injustificada** de los datos personales de los usuarios sin limitación de los periodos de retención. En particular, para el tratamiento de datos personales sensibles, el responsable del tratamiento está obligado a realizar esfuerzos razonables para limitar el periodo de tratamiento al mínimo indispensable.
    - En particular, **no se permite la supresión** de los datos cuando los usuarios dan de baja su línea celular, sino que, sin justificación alguna, se mantendrán durante 6 meses.

- ***Violación al principio de responsabilidad***. La normatividad aplicable en materia de protección de datos personales exige el cumplimiento de una serie de acciones demostrables tendientes a demostrar que el tratamiento de datos que realice el responsable conforme a la normatividad, y, concretamente **en cumplimiento del principio de responsabilidad, previsto en los artículos 14 de la**

LFPDPPP y 74 de la LGPDPPSO, que el responsable del tratamiento realice una **Evaluación de Impacto en la Protección de Datos Personales (en adelante "EIPDP")** cuando exista la probabilidad de que, por su naturaleza, alcance o fines, las operaciones de tratamiento entrañen un alto riesgo para los derechos y las libertades de los titulares de datos personales. Es decir, cuando exista un tratamiento intensivo o relevante de datos personales. En este contexto, se debe recordar que la EIPD:

- Tiene que realizarse de manera previa al tratamiento que se "pretenda poner en operación" que suponga un tratamiento intensivo. Así expresamente el articulo 77 de la LGPDPPSO y el artículo 23 de las Disposiciones EIPDP indican que, los sujetos obligados que realicen una EIPDP, deberán presentarla ante el INAI (o los organismos garantes) cuando menos **treinta días antes** a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, a efecto de que se emita el dictamen correspondiente en los treinta días siguientes (ex art. 78 LGPDPPSO).
- Uno de sus objetivos principales es identificar y describir los altos riesgos potenciales y probables que entrañen los tratamientos intensivos o relevantes de datos personales.
- Se basa en el contraste entre la situación de partida y lo que ocurre una vez que el tratamiento tenga lugar. Ese contraste busca revelar los cambios que se pueden atribuir al tratamiento realizado.
- Derivado de las conclusiones en esa evaluación habrá que decidir si ese tratamiento se puede llevar a cabo, y, en su caso, con qué medidas de seguridad.
- Tal y como el mismo Dictamen de reforma a la LFTR del 16 de abril de 2021 reconoce: *(…)* ***v. Será necesario realizar una evaluación de impacto a la protección de datos personales****, mismo que implica la vulneración de los datos que son confidenciales"*

• El simple hecho de que el Legislador haya sido omiso en realizar una apreciación de proporcionalidad (*test de proporcionalidad*) respecto de la creación del PANAUT en relación con la restricción al derecho humano a la protección de datos personales e instruir al IFT como órgano responsable del tratamiento de datos relativos al PANAUT llevar a cabo una EIPDP, **es violatorio del**

derecho humano de protección de datos personales por incumplimiento al principio de responsabilidad.

- ***Violación al deber de seguridad***. En relación con la violación al deber de seguridad es importante tomar en cuenta lo siguiente:
  - Tanto en la LFPDPPP como en la LGPDPPSO la obligación de seguridad se regula como un deber, y por lo tanto, como una obligación proactiva, preventiva y demostrable para todos los responsables del tratamiento sean estos entes públicos o privados, obligándoles dicho deber a establecer y mantener diversos controles de seguridad administrativos, físicos y técnicos para evitar que la confidencialidad, integridad y disponibilidad de la información se vean comprometidas.
  - En relación con lo anterior no puede pasar desapercibido que los datos personales contenidos en el PANAUT tendrán un valor en el mercado extremadamente alto, por lo que dicha base de datos será susceptible de múltiples ataques en materia de ciberseguridad, en especial si tenemos como referencia los siguientes sucesos que se han presentado, en los últimos años.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucional el Decreto por virtud de que el tratamiento de datos que ordena el Decreto es contrario a lo previsto en el segundo párrafo del artículo 16 de la CPEUM al contravenir los principios de protección de datos personales previstos en la LGPDPPSO.

3. Tercer concepto de invalidez

Como tercer concepto de invalidez, los Senadores integrantes de la LXIV Legislatura sostienen que, en México existe un derecho a la libre disposición del cuerpo que se desprende, por un lado, del derecho a la integridad física y por el otro, del libre desarrollo de la personalidad. Se precisa además que, el derecho a la integridad personal dimana del derecho a la vida y se encuentra contenido en el artículo 29 constitucional, que lo contempla como un derecho irreductible, aun durante un estado de emergencia.

En este sentido, los Senadores integrantes de la LXIV Legislatura señalan lo siguiente:

- De acuerdo con el artículo 5.1 del Pacto de San José, este derecho contempla tres dimensiones: física, psíquica y moral.

- Se tiene entonces que la integridad personal implica que una persona pueda vivir sin que, de forma inesperada, actos arbitrarios de autoridad afecten su salud o habilidades psíquicas.
- La doctrina judicial de esta H. Suprema Corte ha definido que el derecho al libre desarrollo de la personalidad es un área residual de libertad que complementa los derechos básicos que consagra el ordenamiento constitucional; asimismo, dicho derecho se encuentra limitado por los derechos de terceros y el orden público. Así lo han establecido las jurisprudencias 1a./J. 5/2019 (10a.) y 1a./J. 6/2019 (10a.).
- Adicionalmente, el derecho al libre desarrollo de la personalidad posee dos dimensiones: una interna, donde el individuo tiene un rango de acción para materializar sus planes de vida, y otra externa, en la que se protege al individuo de incursiones indebidas a su autonomía personal como lo señala la jurisprudencia 1a./J. 4/2019 (10a.).
- De todo lo anterior se colige que existe un derecho a la libre disposición del cuerpo, que comprende la posibilidad de disponer de nuestro cuerpo de la forma que mejor convenga a nuestros planes de vida.
- Los datos biométricos son parte inmodificable de nuestro cuerpo y por lo tanto, tenemos el derecho de protegerlos y hacer uso de los mismos de la forma en que mejor nos convenga.
- Por ello, los artículos 180 Ter y 180 Quáter de la LFTR, al exigir que los ciudadanos que deseen seguir accediendo a servicios de telefonía móvil deban dar información tan íntima como lo son la voz, la información genética, las huellas, los iris y otros, van en contra de este derecho y son por tanto inconstitucionales.

En este contexto, el Colegio apoya los argumentos de los Senadores integrantes de la LXIV Legislatura y considera que, en efecto, el Decreto vulnera los derechos a la integridad física y por el otro, del libre desarrollo de la personalidad por las siguientes razones:

- Los artículos 180 Bis, 180 Ter, 180 Quater, 180 Septimus último párrafo, 190, fracción VII, Cuarto y Quinto transitorio del Decreto atentan contra el derecho humano al desarrollo, en tanto limitan el desarrollo económico, social, cultural y político en el que puedan realizarse plenamente todos los derechos humanos en contravención a lo dispuesto en el artículo 25, primero a cuarto párrafos de la Constitución Federal y la Declaración sobre el Derecho al Desarrollo de las Naciones Unidas del 4 de diciembre de 1986, ratificada por México.
- El artículo 25, primero a cuarto párrafos de la Constitución Federal, reconoce la vigencia del citado derecho humano supraindividual al desarrollo al establecer, entre otras cosas lo siguiente:

- Que corresponde al Estado la rectoría del desarrollo nacional para garantizar que éste sea integral y sustentable, que fortalezca la Soberanía de la Nación y su régimen democrático y que, mediante la competitividad, el fomento del crecimiento económico y el empleo y una más justa distribución del ingreso y la riqueza, permita el pleno ejercicio de la libertad y la dignidad de los individuos, grupos y clases sociales, cuya seguridad protege esta Constitución. La competitividad se entenderá como el conjunto de condiciones necesarias para generar un mayor crecimiento económico, promoviendo la inversión y la generación de empleo.
- Que el Estado velará por la estabilidad de las finanzas públicas y del sistema financiero para coadyuvar a generar condiciones favorables para el crecimiento económico y el empleo.
- Que el Estado planeará, conducirá, coordinará y orientará la actividad económica nacional, y llevará al cabo la regulación y fomento de las actividades que demande el interés general en el marco de libertades que otorga la Constitución.
- Que al desarrollo económico nacional concurrirán, con responsabilidad social, el sector público, el sector social y el sector privado, sin menoscabo de otras formas de actividad económica que contribuyan al desarrollo de la Nación.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucional el Decreto por virtud de que el tratamiento de datos que ordena el Decreto vulnera los derechos a la integridad física y por el otro, del libre desarrollo de la personalidad.

4. Cuarto concepto de invalidez

Como cuarto concepto de invalidez, los Senadores integrantes de la LXIV Legislatura sostienen que, el Decreto viola el derecho a la identidad previsto en el artículo 4 constitucional y por tanto, debe ser declarado inconstitucional por las razones siguientes:

- Se refiere que, el artículo 4o de la CPEUM establece el derecho a la identidad y se precisa que si bien, el derecho a la identidad parece circunscribirse al reconocimiento de la misma que hace el Estado por medio del registro, este adquiere una faceta diferente cuando lo relacionamos con el artículo 16 constitucional, que establece la base de los datos personales y su régimen de protección.
- Se concluye que los datos personales son en parte un reconocimiento del Estado de la identidad personal, pero también son el rastro irreductible de la

identidad de un individuo y la protección que permite el estado de los datos personales por medio de los derechos ARCO, es en realidad una salvaguarda del derecho a la identidad.

- Los datos personales como conjunto surgen entonces tanto de la libre disposición del cuerpo como de la identidad, pues ambos se encuentran entrelazados de una forma que no siempre resulta fácil hacer una diferencia. En lo que respecta al derecho a la identidad, podemos ver que tiene una doble vertiente: una jurídica, que implica el reconocimiento que hace el Estado del individuo, y otra biométrica, que nace del cuerpo y que se compone de todas las características físicas que permiten distinguirle de otros.
- Al momento en que las reformas a la LFTR no establecen de forma expresa la protección de los datos personales por medio del ejercicio de los derechos ARCO, existe una violación al artículo 4o constitucional. Esta también se actualiza cuando no se cumplen los principios de la LGPDPPSO y cuando no se establece la participación del INAI.
- Por último, el solo hecho que exista una base de datos biométricos sin que una delimitación apropiada tanto en sus fines como en los sujetos que lo pueden utilizar, tenemos una violación constitucional en los términos ya planteados.

Al respecto, este Colegio, apoya los argumentos de los Senadores integrantes de la LXIV Legislatura y considera que, en efecto, como se señaló de forma previa en este documento, el Decreto viola el derecho a la identidad por las razones siguientes:

- El párrafo octavo del artículo 4 constitucional reconoce el derecho a la identidad como un derecho independiente, que identifica a una persona en concreto mediante la suma de distintos factores, refiriéndose al conjunto de elementos que construyen la individualidad de una persona. Este derecho corresponde a todas las persoans y debe ser tutelado y garantizado por el Estado Mexicano, máxime cuando el derecho a la identidad de una persona es un derecho habilitante de otros derechos, y en la actualidad su tutela efectiva enfrenta diversos riesgos y peligros como resultado del acelerado uso de las TIC y la ingente cantidad de datos tratada por las organizaciones tanto públicas como privadas.
- En México, particularmente, **las cifras del denominado delito de "robo o usurpación de identidad**" son muy altas. Por ejemplo, en los primeros tres meses de 2021 se registraron más de 21,500 denuncias por fraude y casi 2,000 por extorsión en el país. En el caso del fraude, las denuncias van al alza desde 2018. En México se han registrado 786 denuncias por falsedad–así clasifica el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) el robo de identidad– en los primeros tres meses de 2021.[81] **Las**

[81] El índice de robo de identidad en México regresó a niveles pre pandemia, CUESTIONE, abril, 2021, disponible en

consecuencias también son muy graves, pero, si además esa usurpación se da sobre datos biométricos, las repercusiones, no solo para los afectados, sino para el entorno y/o mercado donde se produjo, además de las posibles afectaciones consecuentes en otros entornos, pueden ser devastadoras e irreversibles, insistimos, no solo por la afectación real, sino por la imposibilidad de la remediación.

- En definitiva, las amenazas se concretan desde varios frentes:
  - Por el tipo, cantidad, naturaleza y contexto de los datos personales tratados: masivas cantidades de datos sensibles de imposible reparación.
  - Por el númer indefinido de actores que tendrán acceso a dichos datos
  - Por el número de procesos y transferencias diferentes realizadas: recopilación por distintos medios (presencial y digital), desde muy diferentes locaciones (grandes centros de atención a usuarios, "tenditas de la esquina), transferencia desde estos hasta la matriz, y de los diferentes concesionarios y autorizados al Instituto, y de ahí a la multitud de autoridades de investigación y de procuración de justicia, en los tres órdenes de gobierno, que accederían múltiples veces a esta información.
  - La falta de recursos del IFT para esta tarea.
- La gestión del derecho a la identidad está reservado a la Secretaría de Gobernación, a través del RENAPO,[82]como reserva de ley expresa, formal y material, mediante la LGP cuyo artículo 85 establece que la SEGOB tiene a su cargo el registro y la acreditación de la identidad de todas las personas residentes en el país y de los nacionales que residan en el extranjero.
- En consecuencia, de acuerdo a la Jurisprudencia de nuestro máximo tribunal la actuación del IFT y en concreto, la facultad regulatoria de la que le pretendió dotar el legislador con la reforma del 16 de abril de 2021 **debe quedar circunscrita al desarrollo eficiente de la radiodifusión y las telecomunicaciones, quedando excluida de forma contundente y expresa, cualquier regulación distinta de aquellas materias externas a las competencias que en dichas materias que el texto constitucional le ha reservado. Más aún, recordando, que tanto las materias de procuración de justicia como de gestión de la identidad son materias reservadas, respectivamente, a las autoridades de procuración de justicia y a la LGP, respectivamente.**
- El PANAUT genera **una grave afectación al derecho de identidad, de imposible reparación**, porque la no exigencia legal de medidas de cuidado y seguridad (administrativas, físicas y técnicas) para acceder, alimentar y en general tratar los datos biométricos que serán incluidos y accedidos a través del PANAUT por la amplitud de sujetos involucrados en el tratamiento de esos

https://cuestione.com/nacional/robo-identidad-mexico-tarjetas-credito-fraude-datos-usuarios/

[82] Artículo 86.- El Registro Nacional de Población tiene como finalidad registrar a cada una de las personas que integran la población del país, con los datos que permitan certificar y acreditar fehacientemente su identidad.

datos deriva en una amenaza real e inminente que vulnera el derecho de identidad de los usuarios de telefonía móvil.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucional el Decreto por virtud de que el tratamiento de datos que ordena el Decreto vulnera el derecho a la identidad previsto en el artículo 4 constitucional.

5. Quinto concepto de invalidez

Como quinto concepto de invalidez, los Senadores integrantes de la LXIV Legislatura sostienen que, el Decreto viola el derecho a la privacidad previsto en el artículo 16 constitucional y por tanto, debe ser declarado inconstitucional por las razones siguientes:

- Ahora bien, aunado a la identidad y a la libre disposición del cuerpo, existe también en la protección de los datos personales una salvaguarda del derecho a la privacidad.
- La privacidad inicialmente definida por el artículo 16 constitucional que define la privacidad como una vertiente de la seguridad jurídica, donde hay un campo al que las autoridades no pueden entrar de forma arbitraria; esto se traduce no solamente a un espacio físico, sino a ciertos ámbitos de la vida personal.
- Si agregamos lo establecido en el artículo 16 constitucional sobre los datos personales y su protección, podemos ver que el derecho a la privacidad se manifiesta como el de separar aspectos de la vida propia del escrutinio público y la accion gubernamental. Esto implica no solamente un espacio físico como puede ser el hogar, sino tambien a evitar injerencias indebidas al cuerpo y, sobretodo, evitar que se obtenga y/o difunda información sobre el cuerpo y la identidad sin consentimiento.
- Al momento en que se recaban datos biométricos, condicionando la negativa a cederlos a poder acceder a servicios de telefonía, se elimina el principio mas importante de la protección de los datos personales: el consentimiento. Esto implica una injerencia en la vida privada ejercida por la coacción y por lo tanto, es inconstitucional e inconvencional.
- Adicionalmente, la recopilación de datos en la forma que ya se ha dicho en otros conceptos de invalidez, la violación a los principios de la LGPDPPSO, el pésimo diseño institucional del Padrón y otros temas, antes aducidos en los tres agravios anteriores, también nos llevan a concluir que la reforma a la LFTR es inconstitucional e inconvencional por contravenir el derecho a la privacidad.

En relación con lo anterior, este Colegio, considera que el Decreto al ordenar la creación del PANAUT, es una medida desproporcionada y excesiva cuya creación incide directa e injustificadamente en el derecho a la privacidad por las razones siguientes:

- El derecho a la privacidad es un concepto extenso dentro de cual se incluyen otros derechos. Como ejemplo de ello, está el derecho a la intimidad, donde si el primero es el ámbito reservado para cada persona y del que quedan excluidos los demás, el segundo se integra con los extremos más personales de la vida y el entorno familiar. Con base en ello, se puede sostener que.
    - La CPEUM y los tratados internacionales reconocen el derecho de toda persona a la vida privada;
    - El derecho a la vida privada origina la posibilidad de las personas a mantener fuera del conocimiento de los demás (incluidas las autoridades) ciertas manifestaciones o dimensiones de su existencia (conducta, datos, información, objetos) y la correspondiente obligación de que los demás no las invadan sin su consentimiento;
    - La intimidad es una vertiente del derecho a la privacidad;
    - El derecho a la intimidad consiste en el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona.
    - Asimismo, el derecho a la intimidad significa el poder de decisión sobre la publicidad o información de datos relativos a su persona.
- La vida privada comprende a la intimidad como el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona, en consecuencia, se puede afirmar que la vida privada es lo genéricamente reservado y la intimidad es lo radicalmente vedado, como es el caso de los datos biométricos que se pretenden recabar y tratar a través del PANAUT, por lo que, en contraposición con lo dispuesto en la CPEUM y los instrumentos internacionales en materia de derechos humanos suscritos por el Estado Mexicano, se advierte que**, la obtención de datos a partir de lo dispuesto en el Decreto, constituye una intervención arbitraria en el ámbito más privado e íntimo de las personas, sin tomar en consideración que todas las personas gozan de un espacio de proyección de su existencia que quede reservado de la invasión y la mirada de los demás, incluso del Estado**, pues en esta área es que se desarrolla plenamente la personalidad, vulnera los derechos de privacidad y vida privada, protección de datos personales e intimidad.
- La recopilación y el uso de datos personales por las autoridades de investigación y de procuración de justicia en términos de lo previsto en el Decreto, constituye una injerencia en el derecho a la intimidad, la privacidad

y vida privada, y derechos conexos, según lo dispuesto en la CPEUM, el Convenio 108, la LGPDPSO y la LFPDPPP, entre otros instrumentos normativos, y, como tal, **debe basarse en derecho (claro, previsible y accesible)**, **perseguir un objetivo legítimo y limitarse a lo necesario y proporcionado para lograr ese objetivo legítimo.**

- Para que dicha injerencia fuera lícita, todo el tratamiento de datos debería cumplir con los principios **de necesidad, proporcionalidad y limitación de la finalidad.** Esto implica que el tratamiento de datos personales por las autoridades de investigación y de procuración de justicia debe **basarse en fines predefinidos, claros y legítimos establecidos en la ley; debe ser necesario y proporcionado a estos fines legítimos y no debe tratarse de forma incompatible con dichos fines. El tratamiento de datos debe llevarse a cabo de manera legal, justa y transparente. Además, los datos personales tratados por** las autoridades de investigación y de procuración de justicia **deben ser adecuados, pertinentes y no excesivos en relación con los fines. Por último, deben ser precisos y estar actualizados para garantizar la mayor calidad de datos posible.**

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucional el Decreto por virtud de que el tratamiento de datos que ordena el Decreto vulnera el derecho a la privacidad previsto en el artículo 16 constitucional.

6. Sexto concepto de invalidez

Como sexto concepto de invalidez, los Senadores integrantes de la LXIV Legislatura sostienen que, el Decreto viola el derecho humano a la democracia por las siguientes razones:

- El que exista una base de datos biométricos, que pueden ser utilizados para la investigación de cualquier delito, crea un ambiente hostil para el ejercicio de la crítica.
- Donde el PANAUT, creado por el artículo 180 bis de la Ley Federal de Telecomunicaciones habla de “asuntos relacionados con la comisión de delitos” sin especificar, donde las reformas al Código Penal y a la Ley Federal de Telecomunicaciones que instituían el RENAUT eran específicas al secuestro y a la extorsión. Esto resulta violatorio de la libertad de expresar y difundir información, contenida en los artículos 6o y 7o de la Constitución Política de los Estados Unidos Mexicanos.
- POR ESTABLECER UN MECANISMO DE DISUASION PARA PERIODISTAS. La existencia del PENAUT, donde existe una correlación entre las líneas telefónicas móviles y los datos personales más sensibles de

los usuarios, y que la misma se encuentre a disposición de una diversidad de autoridades de seguridad y justicia, para la investigación de cualquier delito en general, constituye un intento de censura previa, establecida en el artículo 13 de la Convención Americana de Derechos Humanos.

  - El Padrón implica mecanismo de censura previa materializado en un efecto disuasor, o chilling effect, lo que constituye a criterio de la Primera Sala, una afectación real y no hipotética. Esto lo ha manifestado en las siguientes tesis aisladas.
  - La interrelación del artículo 180 Bis, respecto a la finalidad del Padrón y la presunción de pertenencia, el 180 Ter, con la inclusión de datos biométricos en el Padrón y la obligatoriedad del registro del 180 Quáter, resulta ser inconstitucional e inconvencional, pues el Estado Mexicano incumple con una obligación fundamental e irreductible de no amedrentar la libre expresión de ideas y el ejercicio de la crítica.

- POR DEBILITAR EL ORDEN DEMOCRATICO. De igual forma, se considera que la existencia del Padrón viene a debilitar la libertad de expresión política y a debilitar el orden democrático. Existe y debe existir una discusión democrática dentro y fuera de campañas, que debe dar lugar a la formación de ideas, la crítica y que, en su momento, permita al electorado tener la mejor información posible para una toma de decisiones.
- Se tiene también que, si la democracia es un derecho humano, lo es también alterar y modificar la forma de gobierno por medio de mecanismos de soberanía popular, entre los que se encuentra la libre expresión de ideas. Por lo tanto, el que exista un padrón de datos biometricos que sirva para amedrentar a opositores politicos, afecta el derecho humano a la democracia.

En relación con lo anterior, desde este Colegio sostenemos, en sintonía con el concepto de invalidez invocado por los aludidos Senadores que, derivado de la violación del derecho de acceso a las TIC como derecho humano habilitante y rector de otros derechos humanos, se impediría el acceso general a los servicios de telecomunicaciones e internet a las personas en cualquier parte del país sin distinción alguna contraviniendo el mandato constitucional de acceso universal a las TIC y las telecomunicaciones según lo dispuesto en la Constitución, por lo que, evidentemente se impediría a las personas expresarse de forma libre a través del uso de las TIC y en consecuencia, participar en la vida democrática del país.

7. Séptimo concepto de invalidez

Como séptimo concepto de invalidez, los Senadores integrantes de la LXIV Legislatura sostienen que, el Decreto viola el derecho humano a la presunción de inocencia por las siguientes razones:

- La creación del PANAUT obliga a los usuarios de líneas de telecomunicación móvil, a entregar a las empresas concesionarias y autorizadas para prestar, o bien, comercializar el servicio, diversos datos personales entre los que se encuentran los datos biométricos; esto con el fin de crear una base de datos en la que se incluirán dichos datos de todos los usuarios en el país.
- El Decreto ordena que en un plazo de dos años a partir de su entrada en vigor, se cancelarán - desconectarán- aquellas líneas de telefonía móvil que no se encuentren dadas de alta en el PANAUT. Esto es, aquellas personas que no estén dispuestas a entregar sus datos personales, incluyendo, los biométricos, no tendrán derecho a seguir utilizando una línea telefónica de este tipo.
- El acceso libre y sin injerencias arbitrarias debe visualizarse desde la perspectiva estatal como una obligación negativa, de no someter o condicionar al gobernado a llevar a cabo acciones injustificadas para tener acceso a una red de telefonía.
- De ninguna manera se justifica en un plano constitucional y convencional que exista un mecanismo como el PANAUT, que se constituya como una auténtica base de datos con la información más sensible de los usuarios de la telefonía móvil en México.
- Un Padrón sin la garantía de qué autoridades serán quienes tengan acceso a la información; sin una regulación sobre los alcances de la protección de los datos biométricos -la información más sensible de una persona-; información que será objeto de investigaciones que presumirán al titular como quien ha cometido conductas que pudieran verse involucradas con la comisión de un delito, cuestión que atenta de manera frontal contra el principio de presunción de inocencia.

En este contexto, coincidimos con los Senadores en que, el Decreto en efecto, viola el derecho de presunción de inocencia toda vez que:

- El Decreto establece un sistema complejo a través del cual los titulares de una línea telefónica ahora se encuentran obligados a registrar información en el PANAUT, no solo información propia, sino también del usuario de la línea en los casos en que éste sea distinto, información que será utilizada como una presunción en materia de procuración de justicia.
    - El artículo 180 Bis, segundo párrafo de la LFTR señala que a partir de la información que se haga constar en el Padrón, se actualizan las siguientes presunciones:

- La existencia de la línea telefónica registrada.
- Que la línea telefónica pertenece a la persona que aparece en el PANAUT como titular o propietaria.
- Los datos que se encuentran registrados en el PANAUT en términos del artículo 180 Ter.
- Que los actos jurídicos que se relacionan con la línea telefónica fueron realizados por su titular, o incluso, por su usuario.

- El hecho de que el artículo 180 Bis se refiera a “actos jurídicos” no otorga garantía alguna a los particulares, sino, los deja en un mayor estado de indefensión, ya que en términos de la legislación no se cuenta con una definición precisa de los actos jurídicos.
- El hecho de que las disposiciones del Decreto incluyan diversas categorías de sujetos que deberán entregar sus datos para conformar el PANAUT y que las normatividades de carácter similar recomiendan separar, tales como los sospechosos, los condenados por una infracción penal, las víctimas o los terceros, entre los que se incluyen los testigos, las personas que posean información o contactos útiles y los cómplices de sospechosos y delincuentes condenados, es suficiente para determinar que el Decreto es contrario al derecho de presunción de inocencia y protección de datos personales.
- La presunción respecto de los datos que se encuentren en el PANAUT tiene como única finalidad entregar la información del padrón a “las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos”, como lo establece el propio artículo 180 Bis, primer párrafo y 180 Septimus, último párrafo de la LFTR.
- La presunción de atribuir determinados actos al titular de la línea, modifica las premisas en las que se basa el principio de presunción de inocencia en tanto que, sin necesidad de probanza alguna se tiene al titular de la línea como responsable de las actuaciones efectuadas a través de ella, pero incluso, en los casos en los que el titular de la línea sea distinto al usuario, se deja a la discrecionalidad de la autoridad atribuir dichas presunciones.
- El Decreto establece en su artículo Sexto transitorio la obligación de los concesionarios y autorizados de telefonía a incentivar la obligación de sus clientes o usuarios de “denunciar en forma inmediata el robo o extravío de sus equipos celulares o de las tarjetas de SIM, así como para prevenir el robo de identidad y el uso ilícito de las líneas telefónicas móviles, así como en los casos que se trate de venta o cesión de una línea telefónica móvil.” Con esto, se pretende trasladar al propio usuario o cliente de telefonía la carga probatoria de acreditar su inocencia mediante la denuncia del robo o extravío de un teléfono celular a fin de pretender desvirtuar la atribución de las conductas relacionadas con la línea.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucional el Decreto por virtud de que el tratamiento de datos que ordena el Decreto vulnera el derecho a la presunción de inocencia previsto en el artículo 20, apartado B fracción I de la CPEUM, 11 de DUDH, 8 de la CADH y el 14.2 del PIDCP, así como los derechos humanos de dignidad humana, libertad, honra, buen nombre previstos en el artículo 1º de la CPEUM, en contra de los titulares y usuarios de telecomunicaciones, en especial de una línea de telefonía móvil.

8. Octavo concepto de invalidez

Como octavo concepto de invalidez, los Senadores integrantes de la LXIV Legislatura sostienen que, el Decreto resulta contrario a las finalidades de la seguridad pública del artículo 21 constitucional por las siguientes razones:

- La existencia de un padrón como el PANAUT es desproporcionado para su propósito, contrario a la legislación existente en materia de datos personales, que recaba y centraliza de forma indebida datos personales sensibles, volviéndolo sujeto a posibles robos; contrario a diversas libertades antes mencionadas, que atenta también contra el orden democrático al establecer un mecanismo amedrentador, resulta contrario a las finalidades de la seguridad pública del artículo 21 constitucional.
- Las reformas que impugnamos son violatorias de la presunción de inocencia y de la finalidad de la función de seguridad pública, contenidas en los artículos 20 y 21 constitucionales por las razones siguientes:
    - El hecho de que se recaben datos personales sensibles con la finalidad de investigar delitos, sin que los mismos se especifiquen, y que no se diga con claridad cuales autoridades pueden acceder al Padrón, es contrario a la presunción de inocencia, pues presupone que potencialmente todos los usuarios pueden, en potencia, cometer un delito. Es decir, se criminaliza a la ciudadanía.
    - Esto queda reforzado con el artículo 180 bis de la LFTR, que establece en su segundo párrafo, que los actos jurídicos que dimanen del uso de un dispositivo de telefonía celular se presumen válidos salvo prueba en contrario. De esta forma, actos criminales llevados a cabo en dispositivos robados se presumen realizados por la persona que tiene registrada la línea.
    - El que se recaben masivamente los datos personales de más de 80 millones de mexicanos, que se puedan usar potencialmente por cualquier autoridad, para investigar cualquier delito y que los actos realizados en los dispositivos registrados a una persona, sean

atribuibles automáticamente a la misma, en su conjunto criminalizan a todas estas personas y contravienen la base de nuestro derecho sancionador. Por tanto, resulta contrario a la Constitución.

- El Padrón es una medida desproporcionada para la finalidad que se realiza, que viene siendo el combate al crimen organizado y al delito. Esto se debe a que, por un lado, recaba datos personales sensibles de una forma que va contraria a la libre disposición del cuerpo y la privacidad, y por el otro, porque va en contra de la lealtad y proporcionalidad de los datos personales, lo que a su vez repercute en las finalidades de la seguridad pública.

En relación con lo anterior, desde este Colegio sostenemos, en sintonía con el concepto de invalidez invocado por los aludidos Senadores y según lo precisado en el primer concepto de invalidez invocado por Senadores, en efecto, el PANAUT se constituye como una medida desproporcionada cuya eficacia empíricamente ha sido desacreditada, máxime cuando las autoridades competentes del país cuentan con diversas herramientas legales a su disposición coom los artículos 252, 252, 291, 301 y 303 del Código Nacional de Procedimientos Penales, el artículo 34 de la Ley de Seguridad Nacional, la Ley de la Guardia Nacional, la fracción I del artículo 190 de la LFTR y la fracción II del artículo 190 de la LFTR.

Por ello, se puede sostener que, la medida no resulta adecuada o racional pues no constituye una medida adecuada para alcanzar el fin perseguido, toda vez que, de un lado, el legislador ni siquiera realizó la previa ponderación de los intereses en pugna. Esto es, omitió definir todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas, y, de otro, porque, de haberlo realizado, habría llegado a la conclusión de que la medida era inadecuada porque todos los resultados empíricos demuestran que la creación de un registro de esta naturaleza no tiene como consecuencia lógica la disminución en los índices delictivos, en particular, respecto de delitos cometidos mediante el uso de dispositivos móviles de comunicación a través de redes de telecomunicaciones, esto es, no existe evidencia de que este tipo de registros influya en la reducción del delito.

9. Noveno concepto de invalidez

Como noveno concepto de invalidez, los Senadores integrantes de la LXIV Legislatura sostienen que, el Decreto constituye una auténtica restricción a los derechos fundamentales, consistente en el condicionamiento del uso de una red de telefonía móvil a que el gobernado entregue sus datos biométricos a las empresas concesionarias y autorizadas para prestar y comercializar el servicio.

Para efectos de demostrar lo anterior, los Senadores integrantes de la LXIV Legislatura aplican el *test* de proporcionalidad señalando lo siguiente:

- NO EXISTE UN FIN CONSTITUCIONALMENTE VALIDO PARA LA REFORMA. La finalidad del PANAUT es contar con una base de datos que contenga los datos personales -incluso los biométricos-, de los titulares y propietarios de una línea de telefonía móvil, para efectos de "colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos en los términos de las disposiciones jurídicas aplicables". La autoridad encargada de instalar, operar, regular y mantener el PANAUT es el IFT, quien se encargará de entregar a las autoridades -sin delimitar a que autoridades se refiere y si requerirá alguna autorización judicial o no- los datos sobre los titulares de las líneas registradas. Incluso, se establece que se presumirá que la línea existe, que el titular es quien está registrado y que los actos jurídicos llevados a cabo relacionados con el contrato de prestación de servicios de telefonía celular se presumen válidos.
- LA MEDIDA NO SATISFACE EL PROPOSITO CONSTITUCIONAL. Esta segunda etapa tiende a analizar si la medida es o no idónea para satisfacer en alguna medida su propósito constitucional; es decir, una cuestión de eficiencia y relación entre la medida y el fin perseguido. Si busca coadyuvar a la reducción en la incidencia delictiva entregando la información a cualquier "autoridad de seguridad y justicia", no solamente no existe un nexo causal entre la medida y el fin buscado, sino que en México se ha demostrado el fracaso de este tipo de mecanismos para tratar de disminuir la incidencia delictiva.
- LA MEDIDA ES INNECESARIA. Actualmente existen previstas en el diversos cuerpos normativos alternativas menos restrictivas al PANAUT. El artículo 190 de la LFTR vigente establece diversas obligaciones en materia de seguridad y justicia a cargo de los concesionarios y autorizados: (i) Colaborar en la localización geográfica de equipos de comunicación móvil; (ii) Conservar un registro y control de comunicaciones que permitan identificar con precisión diversos datos del suscriptor de la línea; y (iii) Conservar la información para su consulta y entrega a autoridades competentes. De lo anterior se desprende que ya existe en el diseño normativo actual diversos mecanismos a través de los cuales las autoridades, en el ámbito de sus competencias, pueden acceder a la información de los suscriptores de telefonía móvil, sin necesidad de allegarse de información sensible y que resultaría a juicio de esta minoría parlamentaria accionante innecesaria para los efectos buscados.
- LA MEDIDA ES DESPROPORCIONADA EN UN SENTIDO ESTRICTO. Finalmente, debemos ponderar los dos principios que compiten en el caso

concreto. En el caso concreto, comparar el grado de intervención en el derecho a las telecomunicaciones -que convive con otros derechos como el de privacidad, a la protección de datos personales, al cuerpo, entre otros-, frente al grado de realización del fin perseguido. Ninguna de las etapas del test de proporcionalidad ha resultado aprobada en este examen. Mucho menos lo hará un examen estricto.

- En ningún Estado constitucional democrático será válido que los gobernados estén obligados a entregar su información más sensible como condición para acceder a una línea telefónica, mucho menos tratándose de que dichos datos serán entregados incluso a autoridades fuera del ámbito de sus atribuciones y competencias, sin ningún tipo de control judicial.

En relación con lo anterior, este Colegio coincide plenamente con los Senadores aludidos respecto de la inconstitucionalidad del Decreto toda vez que este, no resulta garante del principio de proporcionalidad, máxime cuando las medidas ordenadas por el mismo implican una injerencia y limitación injustificada a varios derechos humanos reconocidos en la CPEUM, entre ellos la vida privada, privacidad y protección de datos personales por las siguientes razones:

- **El Decreto y la creación del PANAUT no persiguen una finalidad objetiva y constitucionalmente válida en relación con las limitaciones a otros derechos humanos que impone.** La medida contraviene lo establecido en los artículos 1, 6, 16, 29 de la CPEUM, entre otros, pues de forma clara esta medida incide de forma negativa en los derechos de vida privada, privacidad, protección de datos personales y representa una restricción injustificada, arbitraria e ilícita al derecho de protección de datos personales, entre otros.
- **Incumplimiento del principio de necesidad:** La medida no o resulta adecuada o racional porque no constituye una medida adecuada para alcanzar el fin perseguido, toda vez que, de un lado, el legislador ni siquiera realizó la previa ponderación de los intereses en pugna. Esto es, omitió definir todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas, y, de otro, porque, de haberlo realizado, habría llegado a la conclusión de que la medida era inadecuada porque todos los resultados empíricos demuestran que la creación de un registro de esta naturaleza no tiene como consecuencia lógica la disminución en los índices delictivos, en particular, respecto de delitos cometidos mediante el uso de dispositivos móviles de comunicación a través de redes de telecomunicaciones, esto es, no existe evidencia de que este tipo de registros influya en la reducción del delito como se ha señalado

previamente en el presente documento al citar diversas fuentes de información.

- **Incumplimiento del principio de proporcionalidad:** Han sido diversos los mecanismos que de forma sustitutiva a la creación del Padrón se han recomendado e identificado, siendo la creación del aludido Registro una medida altamente cuestionada de forma previa a su instrumentación, en particular, se ha señalado que:
    - Existencia de mecanismos legales habilitadores para estos fines: además de la legislación general y extensa en materia de seguridad y prevención de delitos y de las facultades de las autoridades competentes, muy en particular respecto del acceso a los datos derivados de los servicios de telecomunicaciones:
    - La posibilidad de acceso no suficientemente controlado a estos tratamientos de datos personales arroja ya en la actualidad serias cifras de abusos por parte de la autoridad.
    - En suma, incluso en la situación actual, ha existido un abuso sistemático y generalizado de las facultades de investigación que invaden la privacidad de personas usuarias de telefonía móvil,
    - Por lo tanto, la ausencia de la creación del Padrón que pretende aprobarse no impide a las autoridades combatir delitos como el de extorsión, sino que constituye un pretexto inaceptable para maquillar la incompetencia de las instituciones de seguridad o intenciones autoritarias, además de que es ilegal.
    - No existe en el país registro alguno, público o privado, que pueda contener mayor cantidad de información sensible de los particulares, además de información personal y de localización, hábitos de consumo, y demás datos personales. El derecho a la privacidad es uno de los pilares de las sociedades democráticas y, como tal, desempeña un papel importante para la realización de los derechos a la libertad de expresión y a opinar sin injerencias. así como a las libertades de reunión y asociación pacíficas.
    - El Padrón genera una grave afectación también en concreto al derecho de identidad, reconocido en el artículo 4º párrafo octavo de la Constitución Federal, de imposible reparación, porque la no exigencia legal de medidas de cuidado para acceder, alimentar y en general tratar los datos biométricos que serán incluidos y accedidos en el Padrón por la diversa multitud de agentes involucrados deriva en una amenaza real y pausible que vulnera el derecho de identidad de los usuarios de telefonía móvil.

Por las razones expuestas, consideramos que es fundamental que ese H. Máximo Tribunal declare inconstitucional el Decreto por virtud de que este constituye una

restricción injustificada e ilegítima a los derechos de privacidad y protección de datos personales previstos en la CPEUM.

10. Solicitud de suspensión

En su demanda de acción de inconstitucionalidad contra el Decreto, los Senadores integrantes de la LXIV Legislatura solicitaron que se suspendieran los efectos de los transitorios del Decreto y que exceptuara la aplicación de los artículos 14, segundo párrafo, interpretado en conjunto con el 59, y el 64 último párrafo, ambos de la Ley Reglamentaria de las Fracciones I y II del artículo 105 de la Ley Reglamentaria de las fracciones I y II de la Constitución Política de los Estados Unidos.

Respecto de este particular y toda vez que ese H. Tribunal ha decretado la negativa a la suspensión solicitada por los Senadores integrantes de la LXIV Legislatura, este Colegio, considera importante precisar que de acuerdo con el artículo 1 de la CPEUM y 64 de la Ley Reglamentaria de las fracciones I y II de la Constitución Política de los Estados Unidos resulta factible conceder la suspensión respecto de normas generales en la acción de inconstitucionalidad “en aquellos casos en que la controversia se hubiera planteado respecto de normas generales que impliquen o puedan implicar la transgresión irreversible de algún derecho humano”, máxime que, como se ha señalado en el presente documento de no suspenderse la aplicación del Decreto se estarían actualizando las violaciones a diversos derechos humanos entre ellos la privacidad, vida privada, protección de datos personales, dignidad, libertad de expresión, presunción de inocencia, acceso a las TIC, legalidad, seguridad jurídica, entre otros.

VIII. Argumentos relacionados con los Recursos de Reclamación 56/2021-CA y 57/2021-CA

En relación con los Recursos de Reclamación 56/2021-CA y 57/2021-CA interpuestos por el INAI y los Senadores integrantes de la LXIV Legislatura con motivo del auto decretado por ese H. Tribunal en el que se negó la suspensión solicitada en las acciones de inconstitucionalidad interpuestas por los sujetos antes referidos, consideramos fundamental someter a un escrutinio amplio dicha determinación por las razones siguientes:

1. Del análisis de la Ley Reglamentaria de las fracciones I y II de la Constitución Política de los Estados Unidos se puede sostener que no existe impedimento normativo en conceder la suspensión respecto de normas generales en la acción de inconstitucionalidad “en aquellos casos en que la controversia se hubiera planteado respecto de normas generales que impliquen o puedan implicar la transgresión irreversible de algún

derecho humano", máxime que, como se ha señalado en el presente documento de no suspenderse la aplicación del Decreto se estarían actualizando las violaciones a diversos derechos humanos entre ellos la privacidad, vida privada, protección de datos personales, dignidad, libertad de expresión, presunción de inocencia, acceso a las TIC, legalidad, seguridad jurídica, entre otros.

2. Se afectaría el núcleo esencial del derecho a la protección de datos personales, mismo que se halla intrínsecamente relacionado con la dignidad y libertad personal.
3. Es procedente la suspensión en contra de normas generales cuando se traten de efectos de realización inminente, teniendo por objetivo preservar la materia del juicio y prevenir daños trascendentes a los derechos humanos.
4. El Decreto produce efectos de realización inminente para los distintos sujetos a los que está dirigida la norma y que incluyen particulares usuarios de líneas celulares, concesionarios, autorizados del servicio de telecomunicaciones y operadores móviles virtuales.
5. No conceder la suspensión solicitada por el INAI y los Senadores de la LXIV Legislatura, podría tener efectos nocivos en el fondo de cada una de las acciones de inconstitucionalidad pues, se daría pie a la emisión de disposiciones secundarias ilícitas y contrarias al principio de reserva de Ley.
6. Existe un riesgo de que se produzcan afectaciones al derecho de acceso a las telecomunicaciones y afectaciones de otros derechos íntimamente relacionados y dependientes de este derecho como la libertad de expresión, la educación, el de libre circulación de ideas y de no injerencia, el de las telecomunicaciones y la radiodifusión como servicios públicos con ciertas características, el de no intervención de comunicaciones privadas, la alfabetización mediática, a los medios de comunicación comunitarios, a los medios de comunicación por parte de pueblos y comunidades indígenas, así como a la accesibilidad a las TIC por personas con discapacidad.
7. Se podría afectar el derecho de acceso a la justicia de las personas, pues el juicio de amparo no podría concebirse como un recurso efectivo contra las disposiciones del Decreto.