

PODER JUDICIAL

SUPREMA CORTE DE JUSTICIA DE LA NACION

SENTENCIA dictada por el Tribunal Pleno de la Suprema Corte de Justicia de la Nación en la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021, así como los Votos Concurrentes de la señora Ministra Loretta Ortiz Ahlf y de los señores Ministros Juan Luis González Alcántara Carrancá, Luis María Aguilar Morales y Presidente Arturo Zaldívar Lelo de Larrea.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Suprema Corte de Justicia de la Nación.- Secretaría General de Acuerdos.

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

PROMOVENTES: INSTITUTO NACIONAL DE
TRANSPARENCIA, ACCESO A LA INFORMACIÓN
Y PROTECCIÓN DE DATOS PERSONALES Y
DIVERSOS SENADORES INTEGRANTES DE LA
LXIV LEGISLATURA

PONENTE: MINISTRA NORMA LUCÍA PIÑA HERNÁNDEZ

SECRETARIOS: EDUARDO ARANDA MARTÍNEZ

Vo. Bo.

Señora Ministra

Ciudad de México. Acuerdo del Tribunal Pleno de la Suprema Corte de Justicia de la Nación correspondiente al **veintiséis de abril de dos mil veintidós**.

VISTOS para resolver en la acción de inconstitucionalidad 82/2021 y su acumulada 86/2021, promovidas, respectivamente, por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y por una minoría de senadores; y

RESULTANDO:

1. **PRIMERO. Presentación de las acciones de inconstitucionalidad.** Mediante escrito remitido el trece de mayo de dos mil veintiuno a través del Sistema Electrónico de la Suprema Corte de Justicia de la Nación, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante "INAI"), por conducto de su Director General de Asuntos Jurídicos, promovió acción de inconstitucionalidad solicitando la invalidez de las normas que a continuación se señalan, emitidas y promulgadas por las autoridades siguientes:

"II. Los órganos legislativo y ejecutivo que emitieron y promulgaron las normas generales impugnadas:

a) Órgano Legislativo: Congreso de la Unión, Cámara de Senadores(...) y, Cámara de Diputados (...).

b) Órgano Ejecutivo: Presidente de los Estados Unidos Mexicanos (...); y Secretaría de Gobernación (...).

III. La norma general cuya invalidez se reclama y el medio oficial en que se publicó: El Decreto por el cual se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno, en particular, sus artículos 15, fracción XLII Bis, 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), 180 Sextus, 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, así como de las omisiones detectadas."

2. El catorce de mayo de dos mil veintiuno, diversos senadores integrantes de la LXIV Legislatura presentaron escrito ante la Oficina de Certificación Judicial y Correspondencia de este Alto Tribunal a través del cual promovieron acción de inconstitucionalidad en los términos siguientes:

"II. ÓRGANOS LEGISLATIVOS Y EJECUTIVO QUE INTERVINIERON EN LA EMISIÓN Y PROMULGACIÓN DE LAS NORMAS CONSTITUCIONALES IMPUGNADAS:

a) ORGANO LEGISLATIVO Y AUTORIDAD EMISORA: Cámara de Diputados del Congreso de la Unión, (...) Cámara de Senadores del Congreso de la Unión, (...).

b) ORGANO EJECUTIVO Y AUTORIDADES PROMULGADORAS: titular del Poder Ejecutivo de la Unión (...).

III. NORMA GENERAL CUYA INVALIDEZ SE RECLAMA Y EL MEDIO OFICIAL EN QUE SE HUBIERE PUBLICADO: el "Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión".

3. **SEGUNDO. Artículos constitucionales y convencionales violados.** En su demanda el INAI consideró que se transgredían 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 Política de los Estados Unidos Mexicanos; 11 de la Convención Americana de Derechos Humanos; 17 del Pacto Internacional de Derechos Civiles y Políticos; 12 de la Declaración Universal de Derechos Humanos; 5, 7 y 8 del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; 1º 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; y 8 y 16 de la Convención de los Derechos del Niño.
4. Por su parte, los senadores integrantes de la LXIV Legislatura estimaron violados los artículos 1º, 14, 16, 72, 74 y 134 de la Constitución Federal.
5. **TERCERO. Conceptos de invalidez.** En su demanda, el INAI expuso los siguientes conceptos de invalidez.

- **Primero.** 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 violan los derechos a la privacidad, protección de datos personales, intimidad e interés superior del menor, 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 debe quedar reservado de la invasión de los demás, incluso del Estado.

La reforma impugnada vulnera estos derechos al ordenar la creación del Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT) que obtendrá, recopilará, almacenará, registrará y conservará los datos personales que en su conjunto dan una radiografía de la vida privada de las personas.

Siendo insuficiente que en el artículo 180 Septimus se prevea que la información del PANAUT será confidencial y reservada, pues la protección constitucional de los datos personales se origina desde su obtención y 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 acorde con el parámetro de regularidad constitucional.

Los preceptos combatidos exigen el tratamiento 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 se vacía de forma absoluta su contenido, al exponer, sin limitación ni justificación legítima, datos personales que se refieren a todas las personas, a sus atributos y a su identidad.

Al respecto, en los asuntos C-293/12 y C-594/12, el Tribunal de Justicia de la Unión Europea examinó la Directiva 2006/24/CE emitida por el Parlamento Europeo que establecía que los proveedores de servicios de comunicaciones telefónicas debían conservar los datos de tráfico y localización relativos a las comunicaciones durante el período establecido en la ley para prevenir y detectar delitos, investigarlos y enjuiciarlos, así como para garantizar la seguridad del Estado; lo cual consideró constituía una injerencia al derecho de protección a los datos personales que no era estrictamente necesaria, pues la medida abarcaba todos los datos de tráfico de telefonía e internet y e incluía de manera generalizada a todas las persona sin establecer ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves.

Además, los datos personales exigidos por el PANAUT pueden permitir el acceso a información u otros datos personales y revelar la geolocalización, datos de cuentas bancarias, implicar robos de identidad y de patrimonio, así como evidenciar las opiniones políticas y creencias religiosas, preferencia sexual, origen racial y étnico, con lo cual el Estado fiscalizaría, revisaría y controlaría el ámbito más privado de las personas.

Así, la información requerida **por sí sola** dará una **radiografía de la vida privada** de las personas (situación patrimonial, económica, de seguridad, integridad) sin una razón legítima. De tal forma que toda apertura en la protección a estos datos desde el momento en que se ordena su recopilación 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 de la Constitución Federal, 11 de la Convención Americana sobre Derechos Humanos, 17 del Pacto Internacional de Derechos Civiles y Políticos, 12 de la Declaración Universal de Derechos Humanos y V de la Declaración Americana de los Derechos y Deberes del Hombre.

Además, se viola el derecho a la intimidad de los ciudadanos, ya que la creación del PANAUT incide en los datos biométricos que son los que permiten identificar de manera unívoca a las personas y además pueden dar cuenta de su origen racial o étnico, entre otras características.

Por otra parte, la reforma conlleva un escenario en el que se permite a diversas autoridades (IFT y autoridades de seguridad pública) y particulares (concesionarios y autorizados) tratar con los datos personales de los usuarios, lo cual supone una amenaza constante al derecho a la privacidad y genera inseguridad para el titular de los datos.

Aunado a ello, el PANAUT se integrará de manera descentralizada, sin que se adviertan mecanismos de protección de datos personales a fin de evitar abusos de las compañías telefónicas y no se puede asegurar que las medidas que se tomen serán eficaces para que los datos personales se integren directamente al padrón, sin que se traten de forma contraria 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, además no se prevén las obligaciones mínimas de cuidado para evitar cualquier pérdida que dé paso a la suplantación o robo de identidad. Por ejemplo, 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, lo cual debilita aún más el derecho a la identidad. Esa amenaza se refuerza porque los distintos actores tendrán acceso los datos que se entreguen, lo que abre la puerta a conductas ilegítimas que terminen en un robo de identidad.

Finalmente, la falta de distinción entre usuarios de telefonía móvil hace presumir que dentro del universo de sujetos obligados a entregar sus datos personales se contempla a los niños y niñas. Su inclusión en el PANAUT implica una violación a sus derechos a la identidad, la privacidad y protección de datos personales, vaciando de contenido al principio de interés superior del menor y dando prevalencia al interés del Estado en perseguir una finalidad que no es legítima. Ello supone una violación de los artículos 4º constitucional, 8 y 16 de la Convención de los Derechos del Niño; y 7 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

- **Segundo.** 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, que regulan la creación del PANAUT son violatorios de los derechos de privacidad y protección de los datos personales en tanto no superan el test de proporcionalidad.

En primer lugar, no se persigue un fin constitucionalmente válido. Para arribar a tal convicción es necesario distinguir entre el fin de la reforma a la Ley Federal de Telecomunicaciones y Radiodifusión y el fin del PANAUT. Así, 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”.

Así, aunque la finalidad del PANAUT es la inhibición de delitos y la colaboración con las autoridades competentes en materia de seguridad y justicia, 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 solo de forma contingente y secundaria, en caso de cometerse un delito, emplear esa información para su persecución.

La finalidad referente al registro y control de las personas a través de un Padrón de líneas telefónicas móviles 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, ello se contrapone a la protección a los derechos a la privacidad, vida privada, intimidad, identidad y protección de los datos personales.

Además, como la medida interviene directamente sobre una vasta nómina de derechos humanos debió cumplir con una finalidad imperiosa desde el punto de vista constitucional y perseguir un objetivo constitucionalmente importante y no solo una finalidad admisible.

El PANAUT 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 PANAUT comprende una lógica circular que se autosatisface a sí misma, en tanto que su razón de ser se colma en su existencia. Por tanto, la reforma impugnada debe declararse inválida pues no conlleva una finalidad constitucionalmente justificada.

Además, en el caso la motivación que ofreció el legislador respecto a la necesidad legislar y crear el PANAUT, referente a la finalidad de perseguir delitos, no cumple el estándar mínimo de motivación reforzada (la indicación precisa de los antecedentes que permitan concluir que lo procedente era crear el PANAUT y la justificación y motivos que llevaron al legislador a actuar en tal sentido).

Por ende, la medida no persigue una finalidad constitucionalmente válida, aunado a que carece de la debida motivación reforzada que se exige cuando se pueden afectar de manera sustantiva derechos y libertades de las personas.

En segundo lugar, la medida no resulta idónea para conseguir su propósito de inhibir delitos.

Durante el proceso legislativo se realizó el “Foro Virtual para el Registro de Usuarios de Telefonía Móvil” en el que diversos expertos expresaron que no había evidencia clara y contundente de que el registro impactara en la reducción de delitos como la extorsión y que la base de datos podría convertirse en un insumo para la delincuencia organizada.

Adicionalmente, la medida no es **idónea**, puesto que no hay relación entre el medio -intervención de derechos a través de recopilación, registros, almacenamiento, uso, transferencia, etc.- y la finalidad consistente en la seguridad pública a través de la colaboración de los delitos de extorsión, dado que no tiene sentido recabar los datos de las líneas postpago cuando la inmensa mayoría de delitos se cometen a través de líneas prepago.

Además, con la medida se conforma una base con los datos de todos los residentes en territorio nacional que cuenten con el servicio de telefonía móvil (veintidós millones de líneas), cuando la cantidad de delitos de extorsión denunciados en México en dos mil veinte fue de ocho mil trescientos ochenta, según cifras del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. De esta forma sólo el 0.0068% de las líneas se encontrarían relacionadas a ese delito, por lo que el crear un padrón nacional no llevará en realidad a ningún fin, salvo a contar con una base que almacene los datos más importantes y sensibles de los residentes del país que tengan dicho servicio.

Al respecto, al resolver los asuntos C-293/12 y C-295/12 el Tribunal de Justicia de la Unión Europea concluyó respecto al tema relativo a la inhibición de los delitos a través de una base de datos, que aun cuando esa medida pretendía contribuir a la lucha contra la delincuencia grave, no exigía ninguna relación entre los datos cuya conservación se establecía y una amenaza para la seguridad pública y, en particular, la conservación no se limitaba a datos referentes a un período temporal o zona geográfica determinados o a personas que pudieran estar implicadas en un delito grave. Razonamiento que motivó, entre otros, la declaratoria de invalidez de la medida cuestionada.

Así, no existe evidencia clara y contundente que el registro impacte en la reducción del delito, por lo que no se supera la etapa de idoneidad.

En tercer lugar la medida no supera la grada de necesidad si se toma en cuenta que de conformidad con el artículo 16 de la Constitución Federal, así como los diversos 189 y 190 de la Ley Federal de Telecomunicaciones y 251, 252, 291, 301 y 303 del Código Nacional de Procedimiento Penales, ya existe la obligación de los concesionarios y autorizados de colaborar en todos los mandamientos de las autoridades y de contar con la tecnología necesaria para cumplir con la entrega de la información que es materia del PANAUT.

Así, 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 aludidos, porque la ordena un juez al caso concreto y requerirá sólo las actuaciones necesarias respecto de las personas investigadas, de tal suerte que no es una medida global para toda la población.

El inhibir la comisión de delitos no depende de la cantidad de datos personales con los que cuente la autoridad, sino que las funciones de seguridad pública, persecución e investigación de los delitos, así como que la administración de justicia se realice de forma eficiente y adecuada.

Finalmente, en cuarto lugar, no se supera la grada de proporcionalidad en sentido estricto pues la medida supone un grado de intervención total en los derechos involucrados dado que se autoriza sin ningún tipo de limitación, a tratar todos los datos personales y sensibles que identifican plenamente a una persona que tenga teléfono móvil, sin que por el contrario se muestre fehacientemente que con ello se inhibirá la delincuencia, en concreto la extorsión.

Por el contrario, en el Foro Virtual para el Registro de Usuarios de Telefonía Móvil se expuso que diversos países han considerado ineficaz la creación de padrones de usuarios para la prevención y persecución de delitos y no hay evidencia de que su implementación haya tenido algún efecto en la disminución de los delitos, tal como sucedió en México con el Registro Nacional de Usuarios de Telefonía Móvil (RENAUT).

- **Tercero.** Los artículos 176, 180 bis, 180 ter, 180 Quáter, 180 Quintes, 180 Sextus, así como los transitorios Tercero, Cuarto y Quinto de la Ley Federal de Telecomunicaciones y Radiodifusión, son contrarios a los artículos 1, 6° y 16 de la Constitución Federal; 5° y 7° del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; 1° del 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; y, 16, 17, 18, 19, 25, 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, pues contravienen los principios de finalidad, licitud, lealtad, proporcionalidad, responsabilidad y seguridad que rigen el tratamiento de datos personales, así como el principio de seguridad jurídica.

En primer lugar, se vulnera el principio de finalidad, de conformidad con el cual los datos personales solo pueden ser tratados para cumplir con la finalidad para la cual se solicitan, la cual debe ser concreta, explícita, lícita y legítima. Ello porque el tratamiento de datos personales que exige el PANAUT ya se realiza por parte de la Secretaría de Gobernación a través del Registro Nacional de Población. Así, si ya existe un sistema que recaba datos personales para fines de identificación, no es válido que el IFT los recabe nuevamente para cumplir esa misma finalidad.

En segundo lugar, se vulnera el principio de licitud que exige que el tratamiento de los datos personales sea acorde con la normativa que rige a la responsable.

Desde una primera vertiente se vulnera dicho principio pues en el caso del IFT sus atribuciones establecidas en el artículo 15 de la Ley Federal de Telecomunicaciones y Radiodifusión guardan una estrecha relación con el mandato de regular y promover la competencia y el desarrollo eficiente de las telecomunicaciones y radiodifusión, mismo que no guarda relación alguna con la inclusión de una fracción XLII Bis en el artículo 15 impugnado, la cual contempla la obligación de operar el PANAUT.

Desde una segunda vertiente del principio de licitud se exige que el tratamiento por parte de la responsable se encuentre apegado a la normativa vigente en materia de datos personales, lo cual no se actualiza pues no se prevé si los concesionarios o sus autorizados deberán conservar o eliminar de sus registros los datos que entreguen al IFT, lo cual también resulta violatorio del principio de seguridad jurídica, en tanto que dejan a los usuarios en incertidumbre porque desconocen quién posee sus datos personales y el tratamiento que se les dará.

En tercer lugar, se vulnera el principio de lealtad porque la regulación del PANAUT permite la manipulación de los datos personales de los usuarios por parte de un número elevado de operadores, creándose un escenario en el que no existe una expectativa razonable de que el tratamiento de su información se apegará a la normativa vigente en materia de datos personales.

En cuarto lugar, se transgrede el principio de proporcionalidad de conformidad con el cual debe existir una relación causa-efecto entre los datos recopilados y las finalidades perseguidas, aunado que los datos que se soliciten deben ser los estrictamente necesarios.

Lo anterior porque la existencia del Registro Nacional de Población a cargo de la Secretaría de Gobernación ya satisface la finalidad genérica de identificación que persigue la creación del PANAUT. Además, respecto a la finalidad concreta de colaborar con las autoridades de seguridad y justicia en la persecución de delitos, lo cierto es que en los artículos 189 y 190, fracciones I, III y IV, de la Ley Federal de Telecomunicaciones y Radiodifusión, ya se prevén obligaciones genéricas a cargo de los concesionarios de proporcionar la información requerida por las autoridades de seguridad, procuración y/o de administración de justicia.

Así, ya existen mecanismos de apoyo que coadyuvan con la finalidad que se busca con la creación del Padrón, por lo que la exigencia de entregar datos biométricos no podría considerarse adecuada y resulta excesiva ya que lejos de cumplir con la finalidad para la cual fue creada, generaría mayores riesgos respecto a la vulneración de los datos personales.

Además, debe tomarse en cuenta el antecedente del RENAUT, diseñado para combatir el secuestro y la extorsión a través del registro de las líneas telefónicas, asociadas al CURP, que encontraba su fundamento en la Ley Federal de Telecomunicaciones y que era operado por la Secretaría de Gobernación, pero cuya normativa se derogó a causa de la desconfianza y tras confirmarse que era ineficaz para alcanzar los objetivos buscados; incluso las bases de datos fueron vulneradas y comercializadas.

En quinto lugar, se vulnera el principio de responsabilidad, pues en los artículos impugnados no se contempla el establecimiento de medidas sustantivas tendentes a garantizar el derecho a la protección de datos personales. De ahí que sea posible que los diversos sujetos responsables carezcan de una capacitación adecuada o desconozcan las obligaciones que deben cumplir para garantizar dicho derecho.

Finalmente, en sexto lugar se vulnera el principio de seguridad porque no se advierte el establecimiento de medidas de seguridad ni 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 Padrón. Por el contrario, el artículo 180 Quintes permite a concesionarios utilizar medios remotos para la recopilación de datos personales, lo cual aumenta el riesgo de su vulneración.

Aunado a ello, se prevé que concesionarios y autorizados corran con los costos implementación, mantenimiento y operación, incluyendo los de conectividad a los servidores del PANAUT sin contemplar que ello no asegura que las dichas medidas cumplan con el principio de responsabilidad y no se establecen mecanismos pertinentes para satisfacer a cabalidad las medidas de seguridad para dicho tratamiento.

- **Cuarto.** Los preceptos impugnados en el tercer concepto de invalidez también transgreden las disposiciones constitucionales y convencionales ahí referidas porque no brindan una protección reforzada a los datos biométricos cuya naturaleza es la de un dato personal sensible y violan el principio de seguridad jurídica.

Si bien no existe una norma vinculante que expresamente disponga que los datos biométricos constituyen datos sensibles, la regulación de diversos ordenamientos internacionales y del derecho comparado da cuenta que reiteradamente se les ha asignado tal carácter.

La posibilidad de individualizar a una persona mediante una propiedad física, fisiológica, de comportamiento o por un rasgo de su personalidad obliga a autorizar una protección reforzada a través del reconocimiento del carácter de datos sensibles.

Aunado a ello, el catálogo de datos personales de carácter sensible enunciados en el artículo 3º, fracción X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados es enunciativo, por lo que permite adicionar nuevos supuestos a los ahí previstos. Además, debe tomarse en cuenta que si los datos biométricos se incluyen en un padrón que los vincula con otros datos personales (como en el caso del PANAUT), el riesgo de individualización aumenta.

En consecuencia, dado que los datos biométricos son datos sensibles requieren una protección reforzada respecto a los principios que rigen el tratamiento de datos personales, aunado a que para su obtención y manejo se requiere la autorización expresa de la persona involucrada (salvo lo previsto en el artículo 22 de la Ley General referida).

Sin embargo, en los preceptos impugnados no se prevén obligaciones complementarias de protección, incluso, no se hace referencia a ningún deber de salvaguarda de los datos que se pretenden recopilar. Aunado a ello, la violación a los principios que rigen el tratamiento de los datos personales aducida en el anterior concepto de invalidez es extensiva respecto de los datos biométricos que tienen el carácter de sensibles.

Esta situación se agrava porque el legislador no estableció qué datos biométricos son los que serán recabados para ser integrados en el PANAUT dejando tal decisión al IFT que no está facultado constitucionalmente para ello, lo cual resulta violatorio del principio de seguridad jurídica y taxatividad legal, consagrado en el artículo 16, párrafo primero, de la Constitución Federal, según el cual las normas deben contener los elementos mínimos para que la autoridad no incurra en arbitrariedades.

- **Quinto.** Los artículos 180 Quintes y 180 Septimus del Decreto impugnado, son contrarios al artículo 16 de la Constitución Federal, al Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados al incluir mecanismos distintos y restrictivos para ejercer los derechos de acceso, rectificación, cancelación y oposición de datos personales (derechos ARCO).

En primer lugar, porque se actualiza una omisión legislativa parcial ya que en los artículos impugnados no señalan los requisitos de presentación de la solicitud, plazos de respuesta y de actuación, ni los medios de impugnación específicos en caso de inconformidad del titular debido la actuación del sujeto obligado responsable. Así, el no incorporar elementos esenciales para ejercer o defender el derecho de protección a datos personales cuando existe una Ley General que los prevé expresamente, genera inseguridad jurídica pues el particular no conoce el marco regulatorio completo que acompaña tal derecho.

En segundo lugar, porque 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, resultando ello contradictorio con el derecho de acceso a datos personales reconocidos por los artículos 8, inciso a), del Convenio 108 y 43 y 44 de la Ley General.

En tercer lugar porque se transgrede el derecho de cancelación ya que si bien el titular de los datos tiene a su alcance la posibilidad de cancelar un número de línea que no reconozca como suyo, 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, lo cual acarrea 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.

Por ende, dado que los preceptos impugnados contienen previsiones sobre derechos ARCO que se ejercen de manera distinta y limitada a lo previsto por la Ley General, deben ser declarados inconstitucionales.

- **Sexto.** Los artículos 15, fracción XLII bis, 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes, 180 Sextus, 180 Septimus, Primero, Segundo, Tercero, Cuarto y Quinto transitorios impugnados transgreden los artículos 6º, Apartado A, fracción VIII, primer y segundo párrafos, 16, segundo párrafo, 28, párrafo quince y 73, fracciones XXIX-O y XXIX-S, de la Constitución Federal porque facultan al IFT para emitir disposiciones en materia de protección de datos personales con motivo de la operación del PANAUT, el cual no tiene atribuciones en esa materia, aunado a que se invade la esfera competencial del INAI.

Con independencia de la inconstitucionalidad de la medida impugnada, lo cierto es que le correspondería al INAI y no al IFT emitir los lineamientos administrativos de carácter general que incidan o puedan tener consecuencia sobre el ejercicio del derecho de protección de datos personales.

Además, 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 legalidad en sus vertientes de reserva de ley y de especialidad, pues la materialización legislativa debe ser acorde con el resto del marco constitucional.

En adición a lo anterior, las normas combatidas transgreden el derecho de protección de los datos personales de todos los ciudadanos ya que sólo un órgano especializado y constitucionalmente habilitado es el competente para salvaguardar y regular, en su caso, el citado derecho.

- **Séptimo.** Los artículos 15, fracción XLII Bis, 180 Ter, 180 Quáter, 180 Quintus, Primero, Cuarto y Quinto transitorios de la Ley Federal de Telecomunicaciones y Radiodifusión son violatorios del artículo 6º, párrafos segundo y tercero, y 7º, párrafos primero y segundo de la Constitución Federal al obligar a todos los usuarios de telefonía móvil a registrarse en el PANAUT, bajo pena de cancelación del servicio.

Con tal medida se viola el derecho de toda persona al acceso a las tecnologías de la información y comunicación (TIC), así como a los servicios de radiodifusión y telecomunicaciones, 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, violándose asimismo la libertad de expresión y la prohibición de la censura.

Las TIC, las telecomunicaciones y el acceso a internet cumplen una función instrumental para el ejercicio de diversos derechos humanos (especialmente considerando que gran parte de la población tiene acceso a Internet a través de su dispositivo móvil) por lo que cualquier medida que restrinja o limite el acceso a estos servicios debe ser analizada en relación con los efectos que pueda generar particularmente respecto a los derechos de acceso a la información y libre expresión.

En ese tenor, la exigencia de requisitos para tener acceso a estos servicios se traduce en la imposición de barreras al ejercicio a los derechos humanos que se ven facilitados por ellos, particularmente los que resultan indispensables para la inserción de la población a la sociedad de la información y el conocimiento.

Aunado a ello, existe todavía un alto porcentaje de la población que, actualmente, no cuenta con acceso a estos servicios, de manera que imponerle a este sector poblacional mayores barreras para su acceso se traduce en una vulneración todavía más grave.

Adicionalmente, el Estado tiene la obligación de garantizar el derecho al libre acceso a las tecnologías de la información y la comunicación, por lo que imponer el requisito de registro con datos personales y datos personales biométricos en el Padrón, so pena de cancelación o negativa de acceso, limita este derecho severamente.

Todo ello también configura una violación al principio de progresividad en su doble vertiente: la prohibición de regresividad y la obligación positiva a cargo del Estado de promover los derechos humanos de manera progresiva y gradual.

El 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. Además, el Alto Tribunal ha reconocido que herramientas de comunicación a través de Internet como, por ejemplo, las redes sociales, son medios para allegarse de información pública.

Finalmente, la medida afecta el derecho a la libertad de expresión pues se genera una censura indirecta, prohibida por el segundo párrafo del artículo 7º constitucional.

- **Octavo.** Los artículos 15, fracción XLII Bis, 180 Ter, 180 Quáter, 180 Quintes, Primero, Cuarto y Quinto transitorios de la Ley Federal de Telecomunicaciones y Radiodifusión son violatorios de la garantía de no retroactividad de la ley en perjuicio de persona alguna, puesto que obran sobre una situación anterior a la norma, respecto de los usuarios que ya contaban con el servicio de telefonía móvil, quienes ahora para poder acceder al servicio deberán proporcionar sus datos al PANAUT. Por ende, se está obrando hacia el pasado sobre el derecho adquirido de acceso a la información a través del servicio de telefonía móvil e internet.
- **Noveno.** Los artículos 176, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes (sic), 180 Sextus, así como transitorios Segundo, Tercero, Cuarto y Quinto impugnados son contrarios a los artículos 17 del Pacto Internacional de Derechos Civiles y Políticos; 11 de la Convención Americana de Derechos Humanos y 12 de la Declaración Universal de Derechos Humanos, al constituir una injerencia arbitraria al derecho a la privacidad, si se atiende a los criterios elaborados por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos para comprobar si una injerencia en tal derecho es legal, contenidos en el informe “El derecho a la privacidad en la era digital”, del que se puede concluir el rechazo a prácticas como la creación del PANAUT, por constituir injerencias arbitrarias y prohibidas por tratados internacionales, al constituir violaciones flagrantes al derecho a la privacidad y su interdependencia con el derecho de protección de datos personales.
- **Décimo.** Los numerales 15, fracción XLII bis, 180 Ter, fracción VI, 180 Quáter, 180 Quintus, 180 Séptimus, último párrafo impugnados, violan las garantías de seguridad y legalidad jurídicas en relación con las técnicas de investigación contenidas en el artículo 16 constitucional, puesto que permiten acceder a datos biométricos sin control judicial.

En términos del artículo 16 constitucional y 252 del Código Nacional de Procedimientos Penales, el requerimiento de datos biométricos exige que un Juez de control lo autorice, previa solicitud del Ministerio Público. No obstante, el artículo 180 Séptimus, último párrafo impugnado no alude a la necesidad de obtener ese control judicial para acceder a los datos biométricos contenidos en el PANAUT, sino que solo establece que si las autoridades conforme a las leyes cuentan con facultades para requerir al IFT, podrán acceder al padrón, sin aclarar si será suficiente con que las leyes las autoricen en términos genéricos, o si se requerirá, además una orden judicial. Por ende, se transgrede el principio de seguridad jurídica y la legalidad en relación con las técnicas de investigación.

Adicionalmente, no existe certeza sobre el número de personas que podrán acceder al padrón, no se define cómo será el acceso a los datos biométricos y a los restantes datos personales, si podrá accederse a todo el padrón o a los datos de solo una persona, ni los requisitos que deben contener los requerimientos de acceso a la información del Padrón cuando debiera exigirse demostrar que la persona respecto de la cual se solicita la información es sujeto de investigación por el delito de extorsión.

Al respecto se recuerda que al resolver los casos C-293/12 y C-594/1, el Tribunal de Justicia de la Unión Europea declaró la invalidez de la Directiva 2006/24/CE, por no prever ningún criterio objetivo que permitiera limitar el número de personas que disponían de la autorización de acceso a los datos conservados ni garantías suficientes, que permitieran asegurar una protección eficaz de esos datos.

- **Décimo primero.** El párrafo segundo del artículo 180 Bis impugnado transgrede el principio de presunción de inocencia, previsto en el artículo 20, apartado B, fracción I, de la Constitución Federal, ya que al disponer que el registro de una línea de telefonía móvil en el PANAUT genera la presunción sobre la existencia de la línea, su titularidad y la validez del contrato de servicio correspondiente, en el supuesto caso que dicha línea sea vinculada como instrumento de un delito, su titular o propietario, de forma inmediata, será considerado como el responsable de ese hecho delictivo.

Con ello se revierte la carga de la prueba que en principio corresponde al acusador en perjuicio del titular de una línea de telefonía.

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 presunción de inocencia como trato procesal.

6. Por su parte, los senadores de la LXIV Legislatura expusieron los siguientes motivos de inconformidad.

- **Primero.** El Decreto impugnado vulnera el principio de legalidad legislativa, en su vertiente dimanada de los artículos 16 y 72 constitucionales, consistente en la debida fundamentación y motivación de los dictámenes legislativos, cuyas deficiencias pueden viciar el debate parlamentario y afectar al proceso legislativo. Así como en su diversa vertiente derivada de los artículos 14 y 72 constitucionales relativa al respeto a las formalidades del procedimiento legislativo.

Ninguna de las dos Cámaras fundamentó y motivó de forma correcta sus dictámenes, aunado a que existieron vicios legislativos en el trámite realizado por el Senado de la República.

El dictamen de la Cámara de diputados adolece de indebida fundamentación porque se omitió basar el dictamen en la legislación aplicable, ya que: 1) deja de considerar que la obligación de los concesionarios de telefonía de colaborar con las autoridades, no implica asumir un costo económico para obtener el equipo necesario con el fin de recabar datos biométricos, ni de realizar actos que serían propios de autoridades; 2) se asigna competencias en materia de datos personales al IFT, lo cual corresponde al INAI; 3) se omite considerar que el régimen legal aplicable es la Ley General de Datos Personales en Posesión de Sujetos Obligados, ya que los concesionarios no recabarán datos para el desempeño de su actividad económica sino para integrar una base de datos en materia de seguridad pública que mantendrá el gobierno; 4) no se aluden a los principios de buen gasto público contenidos en el artículo 134 constitucional, no se toma en cuenta la carga presupuestal que tendría el IFT ni los gastos que irrogarían los concesionarios para recabar los datos; y 5) aunque se menciona una posible violación al principio de presunción de inocencia no se da respuesta a dicha cuestión.

El dictamen también adolece de indebida motivación pues: 1) se analiza de manera sesgada el uso de datos personales; 2) se hizo caso omiso a las opiniones de los expertos durante el “Foro Virtual para el Registro de Usuarios de Telefonía Móviles” respecto a que no había garantía de que con el Padrón disminuyera la comisión de delitos y que se requería un trabajo mayor para limitar a las autoridades su acceso; 3) no se realizó un ejercicio de ponderación para justificar por qué debía prevalecer la seguridad pública sobre la protección de datos personales, sobre todo de datos sensibles; 4) no se ofrece una motivación reforzada tomando en cuenta que existen posibles afectaciones a valores constitucionales y derechos sensibles, que por analogía tendrían el mismo valor que una categoría sospechosa; 5) no se ofrece una justificación sobre porqué a pesar de las medidas ya existentes u otras alternas, se requiere una versión más invasiva del

RENAUT; 6) No se señala una finalidad constitucionalmente válida pues solo se dice que será una herramienta para el combate al delito, sin especificar los ilícitos ni a las autoridades que podrán acceder al padrón y sin incluir al INAI; y 7) No se justifica la idoneidad de lo propuesto, ni se hace referencia a posibles medidas alternativas con los derechos en juego, ni cómo el fin a cumplirse por las iniciativas dictaminadas debe prevalecer sobre cualquier posible afectación.

El dictamen del Senado de la República también adolece de indebida fundamentación y motivación pues: 1) se limita a transcribir el dictamen de la legisladora, centrándose solo en justificar la necesidad de la reforma sin ofrecer un sustento normativo adicional, aunado a que no existe una ponderación entre la seguridad pública y la protección de datos personales; 2) tiene un enfoque punitivo, pues contempla el combate al delito desde la óptica de la sanción (la existencia de un registro invasivo de identidad para poder complementar la persecución del delito), en vez de implementar medidas preventivas o complementarias, como pudiera ser la regulación de las tarjetas SIM; 3) es opaco, ya que se convocó a expertos y no se tomaron en cuenta sus conclusiones; y 4) al igual que el de la legisladora, adolece de la misma falta de justificación de la medida.

Por otra parte, existieron dentro del procedimiento legislativo en la Cámara de Senadores (revisora), diversas violaciones con potencial de invalidar el Decreto impugnado.

Ello porque en la reunión de las Comisiones Unidas de Comunicaciones y Transportes y de Estudios Legislativos de veinticinco de marzo de dos mil veintiuno, únicamente los diputados de la Comisión de Comunicaciones y Transportes votaron el dictamen (aprobándolo por mayoría) en tanto los de la Comisión de Estudios Legislativos no realizaron tal votación, al estar pendiente la resolución sobre una reserva de artículos presentada por un senador, respecto a la cual existió empate de tres votos para determinar si era procedente (lo que no aconteció en la votación respecto a la reserva de la primera comisión, en la que la mayoría votó por la improcedencia de la reserva).

Por tanto, como de conformidad con el artículo 150, numeral 3 del Reglamento del Senado de la República, el dictamen producido bajo la modalidad de trabajo en comisiones unidas debe de ser aprobado en ese acto por la mayoría absoluta de los integrantes de cada una de las comisiones que participan, la votación del dictamen por parte de la Comisión de Comunicaciones y Transportes no se debió llevar a cabo, toda vez que el resultado de la votación de la propuesta por parte de la comisión de Estudios Legislativos, podría influir en la votación de los integrantes del dictamen por parte de ambas comisiones.

En consecuencia, no se respetó el Reglamento del Senado de la República, ni hubo una participación equitativa de todas las fuerzas políticas en el debate y por tanto, la reforma impugnada es inconstitucional.

- **Segundo.** Se vulnera el principio de igualdad porque la reforma entra en contradicción directa con los principios rectores previstos en el numeral 6 del Ley General de Datos Personales en Posesión de Sujetos Obligados (LGDPPSO)¹.

Se transgrede el principio de calidad relativo a que los datos personales deben ser pertinentes y correctos para los fines para los que fueron recabados, pues se busca recabar datos personales sensibles para crear un padrón que en el pasado no ha cumplido su función (antecedente RENAUT), siendo el previsto en la reforma inclusive más invasivo y ambiguo pues no se especifica los delitos para los que puede ser usado, a diferencia del primer padrón.

También se transgrede el principio de responsabilidad porque impone una carga a los operadores de telecomunicaciones y al IFT, que va más allá de su diseño organizacional y que le supone una fuerte obligación económica.

Adicionalmente se vulnera el principio de proporcionalidad porque el daño por el riesgo de filtración de la información del padrón es mayor que el posible bien que puede tener el combate a la delincuencia.

Por tanto, la reforma adolece de una indebida fundamentación y motivación al contravenir directamente la Ley General aludida, transgrediendo así el artículo 16 constitucional.

¹ En realidad, la referencia al artículo 6º y posteriores numerales de este concepto de violación no son de la Ley General, sino que corresponden a la Ley Federal de Protección De Datos Personales en Posesión de los Particulares.

- **Tercero.** La reforma impugnada transgrede el derecho a la “libre disposición del cuerpo”, el cual se desprende de los derechos a la integridad personal y al libre desarrollo de la personalidad, y que reconoce la posibilidad para la persona de disponer de su cuerpo de la forma que mejor convenga a sus planes de vida.

Los datos biométricos son parte inmodificable del cuerpo de la persona y por lo tanto, ésta tiene derecho a protegerlos y a hacer uso de éstos de la forma en que mejor le convenga. Por ello, los artículos 180Ter y 180 Quáter impugnados, al exigir que los ciudadanos que deseen seguir accediendo a servicios de telefonía móvil deben dar información tan íntima como lo son la voz, la información genética, las huellas, los iris y otros, transgreden ese derecho y por ende son inconstitucionales.

- **Cuarto.** La reforma impugnada vulnera el derecho a la identidad, pues no establecen de forma expresa la protección de los datos personales por medio del ejercicio de los derechos ARCO, en contravención al artículo 4º constitucional.

Dicha violación también se genera porque: a) no se cumplen los principios de la LGDPPSO; b) no se establece la participación INAI; y c) existe una base de datos biométricos sin una delimitación apropiada, tanto en sus fines como en los sujetos que lo pueden utilizar.

- **Quinto.** El decreto impugnado transgrede el derecho a la privacidad, reconocido en los artículos 16 constitucional, 11 de la Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos, debido a injerencias indebidas en el cuerpo e identidad de las personas.

Ello porque se condiciona el acceso al servicio de telefonía al otorgamiento de los datos biométricos de la persona con lo cual se elimina el principio de consentimiento que permea en la proyección de los datos personales, generándose una injerencia coactiva en la vida privada.

Además, porque con el PANAUT se crea un sistema de vigilancia permanente e indiscriminado que permite al Estado interferir y monitorear directamente la vida privada de las personas, lo cual es abiertamente contrario a los principios que orientan el funcionamiento de una democracia constitucional contemporánea. Ello sin que la medida conlleve beneficios concretos frente a los derechos sacrificados, garantice la certeza en el uso de los datos, ofrezca un mecanismo de rendición de cuentas para quien reclame abusos, ni prevea esquemas que permitan asegurar que los datos extraídos serán debidamente custodiados y empleados solo con el fin previsto.

La posibilidad de geolocalizar los teléfonos celulares, así como el registro de todas las llamadas y mensajes, genera patrones de uso que permite conocer la vida pública y privada de todos los usuarios, por lo que es crítico que esa información se encuentre debidamente protegida, lo cual pugna con la medida combatida, que hace lo contrario.

En ese sentido al resolver los casos acumulados C-203/15 y C-698/15, el Tribunal de Justicia de la Unión Europea sostuvo que: 1) las medidas encaminadas a registrar indiscriminadamente datos personales de usuarios relacionadas con el uso de tecnologías de la información constituyen una afectación al derecho a la privacidad de las comunicaciones; 2) que la conservación indiscriminada de datos es violatoria de los derechos a la libertad de expresión, a la protección de datos personales, al secreto de las comunicaciones de las personas e incluso al secreto profesional; 3) reconoció la posibilidad de registrar y retener datos pero siempre sujeto a un objetivo concreto y de acuerdo con los estándares de una sociedad democrática; 4) precisó que la salvaguarda de la seguridad pública no puede constituirse en una habilitación amplia de cualquier medida del Estado que afecte los derechos de sus ciudadanos, como cuando la medida afecta a todos los usuarios de líneas telefónicas celulares; y 5) señaló que la persona afectada tiene derecho a ser informada que sus datos fueron consultados.

Adicionalmente, en el diverso caso C-623/17 concluyó que solamente en ocasiones muy especiales es posible que el Estado ordene a un concesionario retener información en forma indiscriminada, precisando que la medida tiene que ser temporal y justificada por cuestiones relacionadas con terrorismo o delincuencia organizada, que la protección del derecho fundamental a la intimidad exige que las excepciones a la protección de datos personales y las restricciones a dicha protección se establezcan sin sobrepasar los límites de lo estrictamente necesario y que en el caso de los mecanismos de recopilación de información indiscriminados y no sujetos a una temporalidad y a un objetivo concreto, la medida es abiertamente contraria a los derechos fundamentales.

Así, al igual que el caso europeo, la reforma impugnada plantea un sistema normativo que recopila datos en forma indiscriminada, sin sujeción a una temporalidad y sin un objetivo concreto, lo cual se traduce en violaciones a la libertad de expresión, a la protección de datos y al derecho a la privacidad de las comunicaciones.

Por otra parte, es cierto que el Tribunal Europeo de Derechos Humanos al resolver el caso *Breyer v. Alemania* determinó que el establecimiento de un padrón que registre a los usuarios de telefonía celular no es per se violatorio de derechos humanos y que Alemania tenía capacidad de recolectar el número de teléfono, el nombre, la dirección y la fecha de nacimiento de las personas usuarias de telefonía móvil de prepago; sin embargo, también reconoció que este tipo de padrones deben estar acompañados de suficientes medidas que garanticen la seguridad de los datos ahí contenidos y de la exigencia de que se garanticen los derechos ARCO.

Sin embargo, a diferencia de la medida impugnada, en el caso alemán no se requerían los datos biométricos de los usuarios y no se generaba un sistema de vigilancia permanente de toda la población usuaria de telefonía celular.

Por otra parte, dada la amplitud de la información recabada, el sistema normativo impugnado permitirá conocer con toda precisión la información de los usuarios, sus costumbres, sus círculos de amistades laborales y personales (toda su vida), por lo que ante tal vigilancia los usuarios tendrán la disyuntiva pues dependiendo de las comunicaciones que entablen pueden verse seriamente afectadas con motivo de la vigilancia permanente, lo cual genera un efecto negativo con relación a los derechos de libertad de expresión y asociación.

- **Sexto.** El Decreto impugnado transgrede el derecho a la libertad de expresión y de difusión de información reconocido en los artículos 6º y 7º de la Constitución Federal, pues la creación de una base de datos biométricos que puede ser utilizados para la investigación de cualquier delito crea un ambiente hostil para el ejercicio de la crítica.

Ello porque no se especifica cuáles son los delitos cuya investigación tendrá relación con el PANAUT, como sí acontecía con el RENAUT, que se limitaba a los ilícitos de secuestro y extorsión.

En ese tenor, los artículos 180 Bis (que establece la finalidad del PANAUT y una presunción de pertenencia de una persona con la línea registrada) en relación con los diversos 180 Ter (que incluye datos biométricos al padrón) y 180 Quáter (obligatoriedad del registro), resultan inconstitucionales e inconvenientes, pues el Estado Mexicano incumple con una obligación de no amedrentar la libre expresión de ideas y el ejercicio de la crítica, constituyéndose así una medida de censura previa, en particular contra periodistas.

Además, la instauración del PANAUT debilita la libertad de expresión política, el orden democrático y afecta los derechos políticos, pues ante la existencia de un padrón de datos biométricos a disposición de las autoridades penales y la previsión del artículo 19 constitucional referente a que los delitos políticos ameritan prisión preventiva, existe un riesgo real y factible para los políticos de oposición de ser acosados por las autoridades, generando un efecto disuasivo.

Además, tomando en cuenta que es mediante el ejercicio de la libertad de expresión que los ciudadanos y líderes de opinión controlan popularmente el ejercicio del poder cuando haya motivos para hacer reclamos legítimos a las autoridades, la medida impugnada se traduce en una afectación al derecho humano a la democracia.

- **Séptimo.** La reforma impugnada también ocasiona una transgresión al derecho de acceso y uso de las telecomunicaciones reconocido en el artículo 6º constitucional, pues se preceptúa que las personas que no estén dispuestas a entregar sus datos personales no tendrán derecho a seguir utilizando una línea telefónica móvil. Así, el Estado incumple su deber de promover el referido derecho el cual debe ser de acceso libre y sin injerencias arbitrarias.

Ponderativamente no resulta válido que el particular deba ceder en su derecho a la privacidad a fin de habilitar el diverso de acceso a las telecomunicaciones, por lo que el Decreto impugnado le impone una carga, que además resulta contraria al principio de interdependencia de derechos, conforme al cual no puede condicionarse el goce de uno a que se ceda en otro.

Adicionalmente se genera un efecto disuasorio para la expansión en el acceso a las telecomunicaciones, pues el artículo 180 Quintes impugnado establece el deber de los concesionarios o autorizados de recabar e ingresar la identidad, datos biométricos y domicilio del usuario, lo que los obliga a desplegar infraestructura para cumplir dicha función, con lo cual el

efecto que se genera es limitar los puntos de venta de telefonía móvil impidiendo que las líneas telefónicas se distribuyan a domicilio, teniendo ello además un impacto más claro tratándose de comunidades apartadas y de escasos recursos, donde se dificultará aún más el acceso a estos servicios.

Del mismo modo, los usuarios se verán inhibidos al tener que entregar sus datos personales para poder acceder a una línea telefónica móvil, generándoles la disyuntiva de elegir entre el derecho a la privacidad de sus datos y el derecho de acceso a las telecomunicaciones.

- **Octavo.** La reforma también atenta contra las garantías institucionales del IFT, pues se establecen obligaciones y facultades a su cargo en materia de datos personales (integrar el PANAUT) que no concuerdan con su diseño institucional y su función primordial de garantizar el desarrollo eficiente de la radiodifusión y las telecomunicaciones, de conformidad con los artículos 6º y 28 constitucionales.

En particular, el Instituto tiene la función de regular, monitorear y vigilar el comportamiento de los concesionarios, pero no el de los usuarios, tan es así que ninguna de sus atribuciones previstas en el artículo 15 de la Ley Federal de Telecomunicaciones y Radiodifusión se refiere a estos últimos, salvo la referente a la institución del PANAUT.

La operación del PANAUT no se ve amparada por las atribuciones del IFT, que se circunscriben a las redes de telecomunicaciones y el espectro radioeléctrico y no a los datos personales sensibles, cuya competencia recae en el INAI, el cual incluso en su comunicado 42/2021, expresó que la reforma podría contraponerse a su mandato de garantizar los derechos contenidos en los artículos 6º y 7º de la Constitución Federal y al favorecimiento del acceso a los servicios de telecomunicaciones.

- **Noveno.** La reforma impugnada es violatoria de principios rectores del procedimiento penal previstos en los artículos 20 y 21 de la Constitución Federal.

En primer lugar, resulta contraria al principio de presunción de inocencia, pues el que se recaben datos personales sensibles con la finalidad de investigar delitos, sin que estos se especifiquen ni se precise con claridad qué autoridades pueden acceder al Padrón, conlleva una omisión que presupone que potencialmente todos los usuarios pueden cometer un delito. Por tanto, se criminaliza a la ciudadanía.

Ello se agrava porque en el segundo párrafo del artículo 180 bis impugnado se prevé que los actos jurídicos que dimanen del uso de un dispositivo de telefonía celular se presumen válidos salvo prueba en contrario, con lo cual los actos criminales realizados en dispositivos robados se presumen realizados por los titulares de las líneas.

Es criterio del Alto Tribunal que el principio de presunción de opera también en situaciones extraprocesales. En ese sentido, no se puede considerar atribuirle a una persona la validez de los actos realizados en el dispositivo registrado a su nombre y vinculado a sus datos personales sensibles, pues se conformaría una prueba preconstituida.

Así, el que se recaben masivamente los datos personales de más de ochenta millones de mexicanos, que se puedan usar potencialmente por cualquier autoridad, para investigar cualquier delito y los actos realizados en los dispositivos registrados a una persona sean atribuibles automáticamente a la misma, tienen un efecto criminalizador respecto de todas estas personas y contravienen la base de nuestro derecho sancionador, siendo por tales razones inconstitucional la reforma impugnada.

En segundo lugar, el PANAUT implica una medida desproporcionada respecto a la finalidad de combate al crimen organizado y al delito. Ello porque se recaban datos personales sensibles afectando “la libre disposición del cuerpo” y privacidad, con lo que se transgreden los principios de lealtad y proporcionalidad de los datos personales y generando una repercusión en las finalidades de la seguridad pública previstas en el artículo 21 constitucional, al ser susceptible de robo.

- **Décimo.** El decreto impugnado contiene una medida que no supera el test de proporcionalidad.

La medida legislativa tiene como finalidad colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos, lo cual impacta los derechos a la privacidad, a la protección de datos personales, a la libre disposición del cuerpo e integridad personal, al acceso y uso de las telecomunicaciones, a la información, a la libertad de expresión, a la inviolabilidad del domicilio y a la presunción de inocencia.

La restricción y limitante a estos derechos se genera porque se condiciona al gobernado a que para acceder y usar una línea de telefonía celular, deba: a) entregar los datos más sensibles - como son los biométricos- a su prestadora del servicio; b) esta última debe entregarlos al IFT, quien los integrará a una base de datos; c) el IFT deberá entregar la información que le sea requerida por otras autoridades competentes en materia de seguridad y justicia; y d) se arroja al gobernado la carga de probar que no es suya la línea que se imputa de su propiedad o titularidad, conforme al registro, así como la invalidez de los actos que se realicen con dicha línea telefónica.

En primer lugar, en la reforma no subyace una finalidad constitucionalmente válida pues si bien se hace mención a los conceptos de seguridad y justicia, no se precisa a qué tipo de seguridad se refiere (nacional, interior o pública) ni qué autoridades serán las involucradas, lo cual abona al debate sobre la delimitación de las fronteras competenciales de las autoridades en materia de seguridad del país. Tales ambigüedades anulan la validez del propósito de creación del PANAUT al permitirse injerencias arbitrarias.

Además, la reforma contiene una cláusula habilitante para que el IFT emita disposiciones administrativas generales respecto al PANAUT, entre ellas, las referentes a la delimitación de los datos biométricos que se integrarán al padrón, lo cual no corresponde a su ámbito competencial sino al del INAI. De igual manera no es factible aceptar que en estas disposiciones se pormenoricen los datos biométricos que integrarán el PANAUT, pues ello debería estar delimitado en la Ley, al constituir una restricción a un derecho humano.

Finalmente, la medida implica una contravención directa a la Constitución Federal respecto a la garantía de inviolabilidad de las comunicaciones, pues se obliga al usuario a entregar sus datos de identificación al IFT sin que medie autorización judicial.

En segundo lugar, la medida no es idónea para satisfacer el propósito constitucional, pues no solamente no existe un nexo causal entre la medida y el fin buscado, sino que en México ya se han probado mecanismos similares, con los mismos fines. Tal es el caso del RENAUT que fracasó e incluso fue derogados al ser mayor el peligro en el que se colocó a la sociedad que la incidencia de esa herramienta en la reducción de los altos niveles de seguridad.

En el caso del RENAUT: a) no se previó validación alguna sobre la veracidad de la información proporcionada, lo cual favorecía la suplantación; b) se pasó por alto que quienes pueden corroborar la información personal de los usuarios son los concesionarios de telefonía móvil; c) No se contaba con un documento de identificación oficial confiable, más que con la credencial para votar, la cual no todos los ciudadanos tienen en virtud de que su obtención no es obligatoria; d) el RENAUT no formó parte de una estrategia nacional de seguridad pública, un esfuerzo que terminó aislado y en manos de una autoridad administrativa; y e) la base de datos fue vulnerada poniendo en riesgo que la información en ella contenida y con ello la integridad de las personas inscritas al conocerse su información personal y sensible.

El PANAUT tiene las mismas debilidades que el RENAUT, por lo que no es un mecanismo idóneo para incidir en la disminución de los altos niveles de seguridad que se han registrado en los últimos años.

Adicionalmente tratándose del caso de líneas de personas morales, éstas quedarán a nombre del representante legal, por lo que si las empresas otorgan dichas líneas a sus empleados o colaboradores la medida no incide en la reducción de la comisión de delitos, pues estos últimos no están registrados en el sistema.

En tercer lugar, la medida no es necesaria pues actualmente ya existen mecanismos a través de los cuales las autoridades competentes pueden allegarse de información de los usuarios de las líneas de telefonía (las previstas en el artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión) sin necesidad de integrar la información sensible, como datos biométricos, a través del PANAUT.

En adición, las deficiencias del RENAUT son replicadas en el PANAUT. Así de buscarse un mecanismo similar para la colaboración de las autoridades en materia de persecución del delito, es necesario que la alternativa prevea: a) las autoridades que estarán involucradas y que podrán acceder a la base de datos; b) autorización de un Juez federal para poder acceder al padrón; c) un sistema efectivo de confirmación de la identidad de la persona titular o propietaria de la línea; d) la inclusión de la base de datos como parte de la estrategia nacional de seguridad, con objetivos y reglas claras sobre su funcionamiento; y e) el catálogo de delitos que ameritarán la injerencia estatal a los datos personales de los titulares de las líneas de telefonía.

En cuarto lugar, la medida no satisface la grada de proporcionalidad en sentido estricto, pues no es válido que los gobernados estén obligados a entregar su información más sensible como condición para acceder a una línea telefónica, mucho menos cuando dichos datos serán entregados incluso a autoridades fuera del ámbito de sus atribuciones y competencias, sin ningún tipo de control judicial.

- Si bien existen autoridades e incluso particulares (instituciones bancarias) que cuentan con los datos biométricos de los gobernados, la diferencia está en que están obligadas a proteger dichos datos, en cambio, el PANAUT está diseñado como un atajo para que esa información sea entregada fuera de cualquier mecanismo de control, lo cual provoca que la medida impugnada que sea desproporcional frente a cualquier supuesto fin legítimo.
7. **CUARTO. Registro y admisión de las acciones de inconstitucionalidad.** Mediante proveído de diecinueve de mayo de dos mil veintiuno, el Presidente de esta Suprema Corte de Justicia de la Nación ordenó formar y registrar la acción de inconstitucional presentada por el INAI con el número de expediente **82/2021** y turnó el asunto a la Ministra Norma Lucía Piña Hernández para fungir como instructora del procedimiento.
 8. En diverso acuerdo de veinte de mayo de dos mil veintiuno, el Presidente de esta Suprema Corte de Justicia de la Nación ordenó formar y registrar la acción de inconstitucional presentada por los senadores de la LXIV Legislatura con el número de expediente **86/2021**, decretó la acumulación del asunto con la diversa acción de inconstitucionalidad **82/2021** y, de la misma manera, lo turnó a la Ministra Norma Lucía Piña Hernández para que instruyera el procedimiento.
 9. Por auto de veintisiete de mayo de dos mil veintiuno, la Ministra instructora admitió las acciones de inconstitucionalidad acumuladas y ordenó dar vista a las Cámaras de Diputados y Senadores del Congreso de la Unión, así como al Poder Ejecutivo Federal, para que rindieran sus respectivos informes. Además, requirió a la Fiscalía General de la República para que formulara pedimento.
 10. **QUINTO. Informe de la Cámara de Senadores del Congreso de la Unión.** Mediante escrito presentado el veintiuno de junio de dos mil veintiuno en la Oficina de Certificación Judicial y Correspondencia de este Alto Tribunal, la Cámara de Senadores, representada por el Senador Oscar Eduardo Ramírez Aguilar, Presidente de su Mesa Directiva, rindió el informe solicitado, sustentando la validez de la normatividad impugnada.
 11. **SEXTO. Informe de la Cámara de Diputados del Congreso de la Unión.** Mediante escrito presentado el veintidós de junio de dos mil veintiuno en la Oficina de Certificación Judicial y Correspondencia de este Alto Tribunal, la Cámara de Diputados, representada por la diputada Dulce María Sauri Riancho, Presidenta de su Mesa Directiva, rindió su informe, sustentando la validez de la normativa impugnada.
 12. **SÉPTIMO. Informe del Poder Ejecutivo Federal.** Mediante escrito presentado el veintidós de junio de dos mil veintiuno en la Oficina de Certificación Judicial y Correspondencia de este Alto Tribunal, Julio Scherer Ibarra, Consejero Jurídico del Ejecutivo Federal rindió informe en representación del Presidente de la República.
 13. **OCTAVO. Pedimento de la Fiscalía General de la República.** La Fiscalía General de la República no formuló pedimento.
 14. **NOVENO. Cierre de instrucción.** Recibidos los informes de las autoridades, formulados los alegatos y encontrándose instruido el procedimiento, mediante proveído de cuatro de agosto de dos mil veintiuno, la Ministra instructora decretó el cierre de la instrucción a efecto de elaborar el proyecto de resolución correspondiente.
 15. **DÉCIMO. Amicus curiae.** Durante la tramitación del expediente, se recibieron en esta Suprema Corte de Justicia de la Nación las promociones que, bajo la figura de *amicus curiae*, presentaron la Comisión de Derechos Humanos de la Ciudad de México; el Ilustre y Nacional Colegio de Abogados; Red en Defensa de los Derechos Digitales; *It Lawyers*, Sociedad Civil; y Centro Iberoamericano para el Desarrollo e Investigación de la Ciberseguridad, Asociación Civil.

CONSIDERANDO:

16. **PRIMERO. Competencia.** Este Tribunal Pleno de la Suprema Corte de Justicia de la Nación, es competente para resolver las presentes acciones de inconstitucionalidad acumuladas de conformidad con lo dispuesto por los artículos 105, fracción II, incisos b) y h) de la Constitución Política de los Estados Unidos Mexicanos y 10, fracción I, de la anterior Ley Orgánica del Poder Judicial de la

Federación, en relación con el punto segundo, fracción II, del Acuerdo General Plenario 5/2013, toda vez que el INAI y una minoría legislativa de la Cámara de Senadores plantean la inconstitucionalidad del Decreto publicado en el Diario Oficial de la Federación de dieciséis de abril de dos mil veintiuno el cual contiene reformas a la Ley Federal de Telecomunicaciones y Radiodifusión.

17. **SEGUNDO. Precisión de normas impugnadas.** De conformidad con los artículos 41, fracción I y 73 de la Ley Reglamentaria de la materia, deben precisarse las normas generales que serán objeto de estudio en la presente acción de inconstitucionalidad.
18. De la lectura integral de las demandas es posible desprender que los accionantes impugnan **la totalidad de las normas** contenidas en el Decreto por el cual se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno.
19. Por un lado, los senadores promoventes hacen valer diversas **violaciones al proceso legislativo**, lo que implica que su impugnación está dirigida –al menos en una parte– a controvertir el proceso de creación del Decreto **en su integridad**.
20. Pero, además, en sus motivos de impugnación ambos accionantes combaten **la totalidad de las normas** que conforman el referido Decreto, pues controvierten el **sistema normativo** a partir del cual se crea y regula el Padrón Nacional de Usuarios de Telefonía Móvil (en adelante “PANAUT”) al estimar que dicha figura transgrede diversos derechos humanos y principios constitucionales.
21. En consecuencia, este Tribunal Pleno tiene por impugnadas **la totalidad de las normas** contenidas en el Decreto por el cual se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno.
22. **TERCERO. Oportunidad.** El primer párrafo del artículo 60 de la Ley Reglamentaria de la materia establece que el plazo para promover la acción de inconstitucionalidad es de treinta días naturales a partir del día siguiente a la fecha en que la norma general sea publicada en el correspondiente medio oficial, tomando en cuenta que, si el último día de dicho plazo fuese inhábil, entonces la demanda podrá presentarse el día hábil siguiente.²
23. En esa tesitura, debe advertirse que el decreto impugnado fue publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno. Así el plazo para controvertirlo corrió del diecisiete de abril al dieciséis de mayo de dicho año, pero como el último día del plazo fue domingo y, por tanto, inhábil, la demanda podía presentarse el lunes diecisiete de mayo siguiente.
24. Por lo tanto, dado que el INAI presentó su demanda el trece de mayo de dos mil veintiuno a través del Sistema Electrónico de la Suprema Corte de Justicia de la Nación y la minoría de senadores hizo lo propio el catorce de dicho mes y año, debe concluirse que ambas promociones resultan oportunas.
25. **CUARTO. Legitimación.** A continuación, se procederá a analizar la legitimación de quienes promueven las presentes acciones, por ser un presupuesto indispensable para su ejercicio.

A) Legitimación del INAI

26. El artículo 105, fracción II, inciso h), de la Constitución Política de los Estados Unidos Mexicanos³, faculta al INAI para promover acción de inconstitucionalidad en contra de leyes que vulneren el derecho al acceso a la información pública y la protección de datos personales, al ser este el órgano garante previsto en el artículo 6º de la Ley Fundamental.

² Artículo 60. El plazo para ejercitar la acción de inconstitucionalidad será de treinta días naturales contados a partir del día siguiente a la fecha en que la ley o tratado internacional impugnado sean publicados en el correspondiente medio oficial. Si el último día del plazo fuese inhábil, la demanda podrá presentarse el primer día hábil siguiente. En materia electoral, para el cómputo de los plazos, todos los días son hábiles.

³ Artículo 105. La Suprema Corte de Justicia de la Nación conocerá, en los términos que señale la ley reglamentaria, de los asuntos siguientes:

[...]

II. De las acciones de inconstitucionalidad que tengan por objeto plantear la posible contradicción entre una norma de carácter general y esta Constitución.

Las acciones de inconstitucionalidad podrán ejercitarse, dentro de los treinta días naturales siguientes a la fecha de publicación de la norma, por:

[...]

h) El organismo garante que establece el artículo 6º de esta Constitución en contra de las leyes de carácter federal y local, así como de tratados internacionales celebrados por el Ejecutivo Federal y aprobados por el Senado de la República, que vulneren el derecho a la información pública y la protección de datos personales. Asimismo, los organismos garantes equivalentes en las entidades federativas, en contra de leyes expedidas por las Legislaturas locales; e

[...]

27. Además, en términos de los artículos 11, primer párrafo, y 59 de la Ley Reglamentaria de la materia⁴, las partes deben comparecer a juicio por conducto de los funcionarios que de conformidad con las normas que los rigen, estén facultados para representarlos.
28. Ahora bien, en el caso, la acción de inconstitucionalidad 82/2021 fue suscrita por **Gonzalo Sánchez de Tagle Pérez Salazar**, en su carácter de Director General de Asuntos Jurídicos del INAI, calidad que acredita con la copia certificada de la credencial expedida por el referido Instituto; funcionario que de conformidad con el artículo 32, fracciones I y II, del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales cuenta con la representación del INAI.⁵
29. Asimismo, es preciso señalar que en términos de los artículos 41, fracción VI, de la Ley General de Transparencia y Acceso a la Información Pública⁶; 35, fracción XVIII, de la Ley Federal de Transparencia y Acceso a la Información Pública⁷; así como 6, 8, 12, fracciones I, IV y XXXV y 18, fracciones IV, XIV, XVI y XXVI del referido Estatuto Orgánico⁸, la promoción de una acción de inconstitucionalidad por parte del INAI debe ser aprobada por la mayoría de los Comisionados del Instituto.
30. Situación que se actualiza en el presente caso, pues el Pleno del INAI aprobó por unanimidad de votos el “Acuerdo ACT-PUB/27/04/2021.03” mediante el cual se instruyó al Director General de Asuntos Jurídicos, como representante legal, para para que interpusiera acción de inconstitucionalidad en

⁴ Artículo 11. El actor, el demandado y, en su caso, el tercero interesado deberá comparecer a juicio por conducto de los funcionarios que, en términos de las normas que los rigen, estén facultados para representarlos. En todo caso, se presumirá que quien comparezca a juicio goza de la representación legal y cuenta con la capacidad para hacerlo, salvo prueba en contrario.

[...]

Artículo 59. En las acciones de inconstitucionalidad se aplicarán en todo aquello que no se encuentre previsto en este Título, en lo conducente, las disposiciones contenidas en el Título II.

⁵ Artículo 32. La Dirección General de Asuntos Jurídicos tendrá las siguientes funciones:

I. Representar legalmente al Instituto en asuntos jurisdiccionales, contencioso-administrativos y ante toda clase de autoridades administrativas y judiciales, en los procesos de toda índole, cuando requiera su intervención y para absolver posiciones;

II. Rendir los informes previos y justificados que en materia de amparo deban presentarse, asimismo, los escritos de demanda o contestación, en las controversias constitucionales o acciones de inconstitucionalidad, promover o desistirse, en su caso, de los juicios de amparo y, en general, ejercitar todas las acciones que a dichos juicios se refieran;

(...).

⁶ Artículo 41. El Instituto, además de lo señalado en la Ley Federal y en el siguiente artículo, tendrá las siguientes atribuciones:

[...]

VI. Interponer, cuando así lo aprueben la mayoría de sus Comisionados, acciones de inconstitucionalidad en contra de leyes de carácter federal, estatal o del Distrito Federal, así como de los tratados internacionales celebrados por el Ejecutivo Federal y aprobados por el Senado de la República, que vulneren el derecho de acceso a la información;

[...]

⁷ Artículo 35. Son atribuciones del Pleno, las siguientes:

[...]

XVIII. Interponer, por el voto de la mayoría de sus integrantes, las controversias constitucionales y acciones de inconstitucionalidad de conformidad con lo previsto en el artículo 105 de la Constitución y su Ley Reglamentaria;

[...].

⁸ Artículo 6. El Pleno es el órgano superior de dirección del Instituto, facultado para ejercer las atribuciones que le establece la Constitución Política de los Estados Unidos Mexicanos, las leyes de la materia y demás disposiciones que resulten aplicables.

Artículo 8. El Pleno es la máxima autoridad frente a los Comisionados en su conjunto y en lo particular, y sus resoluciones son obligatorias para éstos, aunque estuviesen ausentes o sean disidentes al momento de tomarlas.

Artículo 12. Corresponde al Pleno del Instituto:

I. Ejercer las atribuciones que al Instituto le otorgan la Constitución Política de los Estados Unidos Mexicanos, la Ley General, la Ley Federal, la Ley de Protección de Datos Personales, así como los demás ordenamientos legales, reglamentos y disposiciones que le resulten aplicables;

[...]

IV. Interponer las acciones de inconstitucionalidad en contra de leyes de carácter federal o estatal, así como de tratados internacionales que vulneren los derechos de acceso a la información y protección de datos personales, cuando así lo determinen la mayoría de sus integrantes, en términos del artículo 105, fracción II, inciso h de la Constitución Política de los Estados Unidos Mexicanos y su Ley reglamentaria;

[...]

XXXV. Deliberar y votar los proyectos de acuerdos, resoluciones y dictámenes que se sometan a su consideración;

[...].

Artículo 18. Los Comisionados tendrán las siguientes funciones:

[...]

IV. Proponer al Pleno la interposición de acciones de inconstitucionalidad en contra de leyes de carácter federal o estatal, así como de tratados internacionales celebrados por el Ejecutivo Federal y aprobados por el Senado de la República, que vulneren el derecho al acceso a la información pública y la protección de datos personales, en términos de la fracción II, inciso h) del artículo 105 de la Constitución Política de los Estados Unidos Mexicanos;

[...]

XIV. Conocer de los asuntos que le sean sometidos para su aprobación por el Pleno;

[...]

XVI. Suscribir los acuerdos, actas, resoluciones y demás documentos que determine el Pleno;

[...]

XXVI. Someter a consideración del Pleno los proyectos de acuerdos, resoluciones y disposiciones normativas que permitan el cumplimiento de las funciones del Instituto;

[...].

contra del Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación, el dieciséis de abril de dos mil veintiuno.

31. En ese sentido, el Director General de Asuntos Jurídicos del INAI tiene legitimación para promover la acción de inconstitucionalidad 82/2021 en representación del referido Instituto.
32. Similares consideraciones rigieron la decisión de este Tribunal Pleno respecto a la legitimación del INAI al resolver la acción de inconstitucionalidad 127/2020.⁹
33. Finalmente, es de precisar que en la demanda del INAI se hacen valer violaciones a los derechos humanos de acceso a la información y protección de datos personales, por lo que se acredita el requisito material previsto en el artículo 105, fracción II, inciso h), de la Constitución Federal.

B) Legitimación de los senadores integrantes de la la LXIV Legislatura

34. De conformidad con el artículo 105, fracción II, inciso b), de la Constitución General, las acciones de inconstitucionalidad pueden promoverse en contra de leyes federales por el equivalente al treinta y tres por ciento (33%) de los integrantes del Senado de la República.¹⁰
35. A su vez, el artículo 62 de la Ley Reglamentaria de la materia prevé que el escrito inicial de demanda debe estar firmado por cuando menos el treinta y tres por ciento (33%) de los integrantes de los correspondientes órganos legislativos.¹¹
36. Ahora bien, la demanda la suscriben los siguientes cuarenta y ocho senadores:

1. Audelia Esthela Villareal Zavala,	25. Miguel Ángel Osorio Chong
2. Alejandra Noemí Reynoso Sánchez	26. Eruviel Ávila Villegas
3. Nadia Navarro Acevedo	27. Nuvia Magdalena Mayorga Delgado
4. Julen Rementería del Puerto	28. Beatriz Elena Paredes Rangel,
5. José Erandi Bermúdez Méndez	29. Carlos Humberto Aceves del Olmo
6. Jesús Horacio González Delgadillo	30. Heriberto Manuel Galindo Quiñones
7. Martha Cecilia Márquez Alvarado	31. Verónica Martínez García
8. Laura Susana Martínez Cárdenas	32. Claudia Ruíz Massieu Salinas
9. Gina Andrea Cruz Blackledge	33. Ángel García Yáñez
10. Bertha Xóchitl Gálvez Ruiz	34. Jorge Alberto Habib Abimerhi
11. Kenia López Rabadán	35. Sylvana Beltrones Sánchez
12. Josefina Eugenia Vázquez Mota	36. Miguel Ángel Mancera Espinosa
13. José Alfredo Botello Montés	37. Juan Manuel Fócil Pérez
14. María Lilly del Carmen Téllez García	38. Omar Obed Maceda Luna
15. Francisco Javier Salazar Sáenz	39. Marco Trejo Pureco
16. Martha María Rodríguez Domínguez	40. Nancy de la Sierra Arámburo
17. Raúl Paz Alonso	41. Dante Alfonso Delgado Rannau
18. María Guadalupe Murguía Gutiérrez	42. Noé Fernando Castañón Ramírez
19. Damián Zepeda Vidales	43. José Alberto Galarza Villaseñor
20. Roberto Juan Moya Clemente	44. Ruth Alejandra López Hernández
21. Juan Antonio Martín del Campo Martín del Campo	45. Dora Patricia Mercado Castro
22. Indira de Jesús Rosales San Román	46. Indira Kempis Martínez
23. Ismael García Cabeza de Vaca	47. Luis David Ortiz Salinas
24. Gustavo Enrique Madero Muñoz	48. Emilio Álvarez Icaza Longoria

⁹ Resuelta el ocho de julio de dos mil veintiuno. Unanimidad de once votos respecto al apartado de legitimación.

¹⁰ "Artículo 105. (...)

Las acciones de inconstitucionalidad podrán ejercitarse, dentro de los treinta días naturales siguientes a la fecha de publicación de la norma, por:

(...)

d) El equivalente al treinta y tres por ciento de los integrantes de alguna de las Legislaturas de las entidades federativas en contra de las leyes expedidas por el propio órgano;" (...)

¹¹ "Artículo 62. En los casos previstos en los incisos a), b), d) y e) de la fracción II del artículo 105 de la Constitución Política de los Estados Unidos Mexicanos, la demanda en que se ejercite la acción deberá estar firmada por cuando menos el treinta y tres por ciento de los integrantes de los correspondientes órganos legislativos. (...)"

37. Cabe señalar que dichos promoventes acreditaron su calidad de senadores con las copias certificadas de sus constancias de mayoría, así como con el *"ACUERDO DEL CONSEJO GENERAL DEL INSTITUTO NACIONAL ELECTORAL POR EL QUE SE EFECTÚA EL CÓMPUTO TOTAL, SE DECLARA LA VALIDEZ DE LA ELECCIÓN DE SENADORES POR EL PRINCIPIO DE REPRESENTACIÓN PROPORCIONAL Y SE ASIGNAN A LOS PARTIDOS POLÍTICOS NACIONALES ACCIÓN NACIONAL, REVOLUCIONARIO INSTITUCIONAL, DE LA REVOLUCIÓN DEMOCRÁTICA, DEL TRABAJO, VERDE ECOLOGISTA DE MÉXICO, MOVIMIENTO CIUDADANO Y MORENA, LAS SENADURÍAS QUE LES CORRESPONDEN PARA EL PERIODO 2018-2024"* (Acuerdo General INE/CG1180/2018).
38. En ese sentido, si bien de autos se advierte que el senador Emilio Álvarez Icaza Longoria no exhibió su constancia de mayoría, lo cierto es que de la información obtenida de la página oficial de la Cámara de Senadores se advierte que cuenta con dicho carácter,¹² información que debe considerarse como un hecho notorio de conformidad con el artículo 88 del Código Federal de Procedimientos Civiles¹³, de aplicación supletoria a la Ley Reglamentaria de la materia y con lo sostenido por este Alto Tribunal en la tesis de jurisprudencia P./J. 74/2006, de rubro *"HECHOS NOTORIOS. CONCEPTOS GENERAL Y JURÍDICO"*¹⁴.
39. Ahora bien, considerando que de conformidad con el artículo 56 de la Constitución General¹⁵ el Senado de la República se compone por ciento veintiocho integrantes, se colige que los cuarenta y ocho senadores que suscriben la demanda conforman el treinta y siete punto cinco por ciento (37.5%) de dicho órgano legislativo, con lo cual se supera el umbral de treinta y tres por ciento (33%) requerido para la promoción de la acción.
40. En consecuencia, la minoría legislativa accionante cuenta con legitimación para promover la demanda de la acción de inconstitucionalidad 86/2021.
41. **QUINTO. Causas de improcedencia.** A pesar de que, en principio, las partes no hicieron valer de manera expresa causas de improcedencia, lo cierto es que en el informe del Poder Ejecutivo Federal se expone que el INAI carece de legitimación para hacer valer violaciones al proceso legislativo, así como para plantear la vulneración a los principios de interés superior del menor, no retroactividad de la ley en perjuicio de las personas y de presunción de inocencia.
42. Al respecto, cabe precisar que de su escrito inicial de demanda no se advierte que el INAI haya hecho valer violaciones al procedimiento legislativo, aunque sí al resto de principios que se mencionan.
43. No obstante, este Tribunal Pleno estima que no asiste la razón al Ejecutivo Federal pues la legitimación del Instituto promovente, de conformidad con el artículo 105, fracción II, inciso h) constitucional, debe evaluarse en función del acto que se impugna y su vinculación con la afectación a los derechos humanos de acceso a la información y protección de datos personales, **no en función de los argumentos que se hacen valer para proteger tales derechos.**
44. En esa tesitura, el aspecto fundamental que en el caso concreto determina la legitimación del INAI es que se impugna el Decreto por el cual se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación el

¹² Consultable en el enlace: <https://www.senado.gob.mx/64/senador/1081>

¹³ ARTICULO 88.- Los hechos notorios pueden ser invocados por el tribunal, aunque no hayan sido alegados ni probados por las partes.

¹⁴ De texto: "Conforme al artículo 88 del Código Federal de Procedimientos Civiles los tribunales pueden invocar hechos notorios, aunque no hayan sido alegados ni probados por las partes. Por hechos notorios deben entenderse, en general, aquellos que por el conocimiento humano se consideran ciertos e indiscutibles, ya sea que pertenezcan a la historia, a la ciencia, a la naturaleza, a las vicisitudes de la vida pública actual o a circunstancias comúnmente conocidas en un determinado lugar, de modo que toda persona de ese medio esté en condiciones de saberlo; y desde el punto de vista jurídico, hecho notorio es cualquier acontecimiento de dominio público conocido por todos o casi todos los miembros de un círculo social en el momento en que va a pronunciarse la decisión judicial, respecto del cual no hay duda ni discusión; de manera que al ser notorio la ley exime de su prueba, por ser del conocimiento público en el medio social donde ocurrió o donde se tramita el procedimiento." Novena Época, Semanario Judicial de la Federación y su Gaceta. Tomo XXIII, Junio de 2006, página 963. Registro 174899.

¹⁵ Artículo 56. La Cámara de Senadores se integrará por ciento veintiocho senadoras y senadores, de los cuales, en cada Estado y en la Ciudad de México, dos serán elegidos según el principio de votación mayoritaria relativa y uno será asignado a la primera minoría. Para estos efectos, los partidos políticos deberán registrar una lista con dos fórmulas de candidatos. La senaduría de primera minoría le será asignada a la fórmula de candidaturas que encabece la lista del partido político que, por sí mismo, haya ocupado el segundo lugar en número de votos en la entidad de que se trate.

Las treinta y dos senadurías restantes serán elegidas según el principio de representación proporcional, mediante el sistema de listas votadas en una sola circunscripción plurinominal nacional, conformadas de acuerdo con el principio de paridad, y encabezadas alternadamente entre mujeres y hombres cada periodo electivo. La ley establecerá las reglas y fórmulas para estos efectos

dieciséis de abril de dos mil veintiuno, por virtud del cual se expidió un **sistema normativo** que crea y regula el "PANAUT", el cual estima dicho promovente genera un impacto en la protección de los derechos humanos de acceso a la información y protección de datos personales.

45. En consecuencia, el hecho de que se hagan valer diversos tipos de argumentos como la vulneración a los principios de interés superior del menor, retroactividad, presunción de inocencia, etc., ello en nada contradice la legitimación previamente reconocida, pues, además de lo ya expresado, es claro que dichos argumentos se relacionan con la protección del derecho a la privacidad, la intimidad y la protección de los datos personales, en tanto a través de ellos se pretende demostrar la invalidez de las normas que los impactan.
46. Por estas consideraciones, tal y como se adelantó, este Tribunal Pleno considera que es **infundada** la causal de improcedencia formulada por el Ejecutivo Federal, pues el INAI cuenta con la legitimación necesaria para promover la presente acción de inconstitucionalidad.
47. En consecuencia, al no haberse planteado una diversa causal de improcedencia ni advertirse de oficio alguna distinta, este Tribunal Pleno procede al análisis de fondo del asunto.

ESTUDIO DE FONDO

48. **SEXTO. Violaciones al proceso legislativo.** Este Tribunal Pleno ha sostenido que en las acciones de inconstitucionalidad debe privilegiarse el análisis de los conceptos de invalidez en los que se hagan valer violaciones al procedimiento legislativo que dio lugar a la norma o normas impugnadas, puesto que, de resultar fundados, ello daría lugar a la invalidación total de tales preceptos, siendo por tanto innecesario ocuparse de los vicios de fondo.¹⁶
49. En ese sentido, se advierte que en su primer concepto de invalidez los senadores promoventes hacen valer dos violaciones al procedimiento legislativo que dio origen al Decreto impugnado: la primera relacionada con la vulneración a los principios de fundamentación y motivación de los actos legislativos, concretamente de los dictámenes elaborados por las cámaras de origen y revisora; y la segunda relacionada con la existencia de irregularidad en la aprobación del dictamen por parte de las comisiones unidas de Comunicaciones y Transportes y de Estudios Legislativos, en el seno de la Cámara de Senadores.
50. En esa tesitura, a fin de poder dar respuesta a este planteamiento resulta conveniente, en primer término, analizar la doctrina que ha desarrollado este Alto Tribunal con relación a la evaluación de las violaciones al proceso legislativo, para, posteriormente, proceder al estudio concreto de las violaciones alegadas por los accionantes.

I. Doctrina de la Suprema Corte de Justicia de la Nación sobre las violaciones al proceso legislativo

51. Este Alto Tribunal ha sostenido que la violación a las formalidades del procedimiento legislativo debe abordarse desde la consideración de las premisas básicas en las que se asienta la democracia liberal representativa elegida como modelo de Estado, de acuerdo con los artículos 39, 40 y 41 de la Constitución General, por lo que la evaluación del potencial invalidante de dichas irregularidades debe intentar el equilibrio entre dos principios: por un lado, el de economía procesal, que apunta a la necesidad de no reponer de manera innecesaria etapas procedimentales, cuando ello no redundaría en un cambio sustancial de la voluntad parlamentaria expresada y, por tanto, a la necesidad de no dar efecto invalidante a todas y cada una de las irregularidades procedimentales identificables en un caso concreto; y, por otro, el de equidad en la deliberación parlamentaria, que apunta, por el contrario, a la

¹⁶ Registro digital: 17088, Instancia: Pleno, Novena Época, Materias(s): Constitucional, Tesis: P./J. 32/2007, Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXVI, Diciembre de 2007, página 776, Tipo: Jurisprudencia
ACCIÓN DE INCONSTITUCIONALIDAD EN MATERIA ELECTORAL. LAS VIOLACIONES PROCESALES DEBEN EXAMINARSE PREVIAMENTE A LAS VIOLACIONES DE FONDO, PORQUE PUEDEN TENER UN EFECTO DE INVALIDACIÓN TOTAL SOBRE LA NORMA IMPUGNADA, QUE HAGA INNECESARIO EL ESTUDIO DE ÉSTAS. El Tribunal Pleno de la Suprema Corte de Justicia de la Nación en la jurisprudencia P./J. 6/2003, publicada en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVII, marzo de 2003, página 915, sostuvo que en acción de inconstitucionalidad en materia electoral debe privilegiarse el análisis de los conceptos de invalidez referidos al fondo de las normas generales impugnadas, y sólo en caso de que resulten infundados deben analizarse aquellos en los que se aduzcan violaciones en el desarrollo del procedimiento legislativo originó a la norma general impugnada. Sin embargo, una nueva reflexión sobre el tema conduce a apartarse de la jurisprudencia citada para establecer que la acción de inconstitucionalidad es un medio de control abstracto, cuando se hagan valer violaciones al procedimiento legislativo que dio origen a la norma general impugnada, éstas deberán analizarse en primer término, ya que, de resultar fundadas, por ejemplo, al trastocar valores democráticos que deben privilegiarse en nuestro sistema constitucional, su efecto de invalidación será total, siendo, por tanto, innecesario ocuparse de los vicios de fondo de la ley impugnada que, a su vez, hagan valer los promoventes.

necesidad de no considerar automáticamente irrelevantes todas las infracciones procedimentales que se produzcan en una tramitación parlamentaria que culmina con la aprobación de una norma mediante una votación que respeta las previsiones legales al respecto.¹⁷

52. Lo anterior significa que no cualquier violación del procedimiento legislativo es susceptible de invalidar la ley analizada, sino sólo aquellas que trasciendan a su calidad democrática, ya sea porque lesionen el principio de participación de todas las fuerzas políticas representativas en condiciones de igualdad, o bien porque desconozcan el principio de deliberación democrática, es decir, porque afecten las condiciones para que pueda desarrollarse una genuina deliberación política.
53. Sobre el particular, es importante señalar que la democracia representativa es un sistema político valioso no solamente porque en su contexto las decisiones se toman por una mayoría, sino porque aquello que se somete a votación ha podido ser objeto de deliberación por parte tanto de las mayorías como de las minorías políticas. Es precisamente el peso representativo y la naturaleza de la deliberación pública lo que otorga todo su sentido a la reglamentación del procedimiento legislativo y lo que califica una decisión como democrática.
54. En efecto, la adopción de decisiones por mayoría, regla básica que permite resolver en última instancia las diferencias de opinión, **es una condición necesaria de la democracia, pero no suficiente**. No todo sistema que adopta la regla de la mayoría es necesariamente democrático. Junto a la regla de la mayoría, hay que tomar en consideración el valor de la representación política, material y efectiva de los ciudadanos que tienen todos y cada uno de los grupos políticos con representación parlamentaria, así sean los minoritarios, y el modo en que la aportación de información y puntos de vista por parte de todos los grupos parlamentarios contribuye a la calidad de aquello que finalmente se somete a votación.
55. En ese sentido, si el simple respeto a las reglas de votación por mayoría podría convalidar cualquier desconocimiento de las reglas que rigen el procedimiento legislativo previo, la dimensión deliberativa de la democracia carecería de sentido, precisamente porque las minorías por su propia naturaleza están predestinadas a no imponerse en la votación final, por tanto, es aquí donde cobran toda su importancia las reglas que garantizan la participación efectiva de tales minorías.
56. En consecuencia, debe resaltarse que el órgano legislativo, antes de ser un órgano decisorio, **tiene que ser un órgano deliberante**, donde encuentren cauce de expresión las opiniones de todos los grupos, tanto los mayoritarios como los minoritarios. Lo anterior es así porque las reglas que disciplinan el procedimiento legislativo protegen el derecho de las minorías a influir y moldear, en el transcurso de la deliberación pública, aquello que va a ser objeto de la votación final y, por tanto, otorga pleno sentido a su condición de representantes de los ciudadanos.
57. Así, para determinar si las violaciones al procedimiento legislativo tienen un potencial invalidante, es necesario evaluar el cumplimiento de una serie de estándares, los cuales tienen como objetivo precisamente el poder determinar si las irregularidades denunciadas impactan o no en la calidad democrática de la decisión final. Dichos parámetros son los siguientes:
 - 1) El procedimiento legislativo debe respetar el derecho a la participación de todas las fuerzas políticas con representación parlamentaria, en condiciones de libertad e igualdad, es decir, resulta necesario que se respeten los cauces que permiten tanto a las mayorías como a las minorías parlamentarias expresar y defender su opinión en un contexto de deliberación pública, lo cual otorga relevancia a las reglas de integración y quórum en el seno de las Cámaras y a las que regulan el objeto y el desarrollo de los debates;

¹⁷ Semanario Judicial de la Federación, Registro digital: 169493, Instancia: Pleno, Novena Época, Materias(s): Constitucional, Tesis: P. XLIX/2008, Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXVII, Junio de 2008, página 709, Tipo: Aislada FORMALIDADES DEL PROCEDIMIENTO LEGISLATIVO. PRINCIPIOS QUE RIGEN EL EJERCICIO DE LA EVALUACIÓN DE SU POTENCIAL INVALIDATORIO. Cuando en una acción de inconstitucionalidad se analicen los conceptos de invalidez relativos a violaciones a las formalidades del procedimiento legislativo, dicho estudio debe partir de la consideración de las premisas básicas en las que se asienta la democracia liberal representativa como modelo de Estado, que es precisamente el acogido por la Constitución Política de los Estados Unidos Mexicanos en sus artículos 39, 40 y 41. A partir de ahí, debe vigilarse el cumplimiento de dos principios en el ejercicio de la evaluación del potencial invalidatorio de dichas irregularidades procedimentales: el de economía procesal, que apunta a la necesidad de no reponer innecesariamente etapas procedimentales cuando ello no redundaría en un cambio sustancial de la voluntad parlamentaria expresada y, por tanto, a no otorgar efecto invalidatorio a todas y cada una de las irregularidades procedimentales identificables en un caso concreto, y el de equidad en la deliberación parlamentaria, que apunta, por el contrario, a la necesidad de no considerar automáticamente irrelevantes todas las infracciones procedimentales producidas en una tramitación parlamentaria que culmina con la aprobación de una norma mediante una votación que respeta las previsiones legales al respecto.

- 2) El procedimiento deliberativo debe culminar con la correcta aplicación de las reglas de votación establecidas; y,
 - 3) Tanto la deliberación parlamentaria como las votaciones deben ser públicas.¹⁸
58. Cabe precisar que esta doctrina constitucional ha sido reiterada por este Tribunal Pleno en múltiples precedentes, siendo los más recientes las acciones de inconstitucionalidad 36/2013¹⁹, 121/2017 y sus acumuladas 122/2017, 123/2017 y 135/2017²⁰, 43/2018²¹, y 121/2020 y su acumulada 125/2020²², así como las controversias constitucionales 34/2014²³, 41/2014²⁴ y 63/2016²⁵.

II. Falta de fundamentación y motivación del acto legislativo

59. Como se mencionó anteriormente, la minoría parlamentaria argumenta que los dictámenes emitidos tanto por la Cámara de Diputados como por la Cámara de Senadores no estuvieron **debidamente fundados y motivados**, pues no se dieron razones suficientes para justificar la afectación ocasionada a los derechos humanos a la privacidad, la intimidad y la protección de los datos personales, así como diversos principios como el interés superior del menor y la presunción de inocencia. Para sustentar dicha afirmación, hacen valer diversos argumentos los cuales pueden englobarse de la siguiente manera:
- a) Cámara de Diputados. 1) el dictamen es omiso en aplicar la legislación correspondiente; 2) se analiza de manera sesgada el tema de la protección de los datos personales, haciendo caso omiso a las opiniones de los expertos; 3) no se justifica el por qué debe prevalecer la seguridad pública sobre la protección de estos datos; 4) no se brinda una motivación reforzada que justifique las posibles afectaciones a valores constitucionales y derechos sensibles; 5) no se ofrece una justificación sobre por qué a pesar de las medidas ya existentes u otras alternas, se requiere una versión más invasiva que el RENAUT; 6) no se señala una finalidad constitucionalmente válida, no se justifica la idoneidad de la medida, ni se ofrece un análisis de las medidas alternativas; 7) se asignan competencias que son ajenas al objeto constitucional del Instituto Federal de Telecomunicaciones ("IFT") y, por el contrario, se

¹⁸ Semanario Judicial de la Federación y su Gaceta, Novena Época, Pleno, tesis aislada, tomo XXVII, junio de 2008, P. L/2008, página 717, registro digital 169437.

PROCEDIMIENTO LEGISLATIVO. PRINCIPIOS CUYO CUMPLIMIENTO SE DEBE VERIFICAR EN CADA CASO CONCRETO PARA LA DETERMINACIÓN DE LA INVALIDACIÓN DE AQUÉL. Para determinar si las violaciones al procedimiento legislativo aducidas en una acción de inconstitucionalidad infringen las garantías de debido proceso y legalidad contenidas en la Constitución Política de los Estados Unidos Mexicanos y provocan la invalidez de la norma emitida, o si por el contrario no tienen relevancia invalidatoria de esta última, por no llegar a trastocar los atributos democráticos finales de la decisión, es necesario evaluar el cumplimiento de los siguientes estándares: 1) El procedimiento legislativo debe respetar el derecho a la participación de todas las fuerzas políticas con representación parlamentaria en condiciones de libertad e igualdad, es decir, resulta necesario que se respeten los cauces que permiten tanto a las mayorías como a las minorías parlamentarias expresar y defender su opinión en un contexto de deliberación pública, lo cual otorga relevancia a las reglas de integración y quórum en el seno de las Cámaras y a las que regulan el objeto y el desarrollo de los debates; 2) El procedimiento deliberativo debe culminar con la correcta aplicación de las reglas de votación establecidas; y, 3) Tanto la deliberación parlamentaria como las votaciones deben ser públicas. El cumplimiento de los criterios anteriores siempre debe evaluarse a la vista del procedimiento legislativo en su integridad, pues se busca determinar si la existencia de ciertas irregularidades procedimentales impacta o no en la calidad democrática de la decisión final. Así, estos criterios no pueden proyectarse por su propia naturaleza sobre cada una de las actuaciones llevadas a cabo en el desarrollo del procedimiento legislativo, pues su función es ayudar a determinar la relevancia última de cada actuación a la luz de los principios que otorgan verdadero sentido a la existencia de una normativa que discipline su desarrollo. Además, los criterios enunciados siempre deben aplicarse sin perder de vista que la regulación del procedimiento legislativo raramente es única e invariable, sino que incluye ajustes y modalidades que responden a la necesidad de atender a las vicisitudes presentadas en el desarrollo de los trabajos parlamentarios, como por ejemplo, la entrada en receso de las Cámaras o la necesidad de tramitar ciertas iniciativas con extrema urgencia, circunstancias que se presentan habitualmente. En este contexto, la evaluación del cumplimiento de los estándares enunciados debe hacerse cargo de las particularidades de cada caso concreto, sin que ello pueda desembocar en su final desatención.

¹⁹ Bajo la Ponencia de la Ministra Norma Lucía Piña Hernández, fallada el trece de septiembre de dos mil dieciocho.

²⁰ Bajo la Ponencia del Ministro Gutiérrez Ortiz Mena, fallada el dieciséis de enero de dos mil veinte por unanimidad de once votos de las Ministras y los Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá, Esquivel Mossa, Franco González Salas, Aguilar Morales, Pardo Rebolledo, Piña Hernández, Ríos Farjat, Laynez Potisek, Pérez Dayán y Presidente Zaldívar Lelo de Larrea.

²¹ Bajo la Ponencia del Ministro Pérez Dayán, fallada el veintisiete de julio de dos mil veinte, bajo la por mayoría de nueve votos de las Ministras y los Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá, Franco González Salas, con consideraciones adicionales y anuncia voto concurrente, Aguilar Morales, Pardo Rebolledo, Piña Hernández, contra de algunas consideraciones y anuncio de voto concurrente, Ríos Farjat, Laynez Potisek y Pérez Dayán. La Ministra Esquivel Mossa y el Ministro Presidente Zaldívar Lelo de Larrea votaron en contra.

²² Bajo la Ponencia del Ministro Gutiérrez Ortiz Mena, fallada el veintidós de abril de dos mil veintiuno por mayoría de nueve votos de las Ministras y los Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá, Franco González Salas, Aguilar Morales, Pardo Rebolledo, Piña Hernández, Ríos Farjat, Laynez Potisek y Pérez Dayán. Votaron en contra la Ministra Esquivel Mossa y el Ministro Zaldívar Lelo de Larrea.

²³ Bajo la Ponencia del Ministro José Fernando Franco González Salas (en su ausencia hizo suyo el asunto la señora Ministra Margarita Beatriz Luna Ramos), fallada el seis de octubre de dos mil quince.

²⁴ Bajo la Ponencia del Ministro José Fernando Franco González Salas (en su ausencia hizo suyo el asunto la señora Ministra Margarita Beatriz Luna Ramos), fallada el veintinueve de septiembre de dos mil quince.

²⁵ Bajo la Ponencia de la Ministra Esquivel Mossa, fallada el veintitrés de septiembre de dos mil diecinueve por mayoría de nueve votos de la Ministra y los Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá, Franco González Salas, Aguilar Morales, Pardo Rebolledo, Piña Hernández, Medina Mora, Laynez Potisek y Pérez Dayán. Votaron en contra la Ministra Esquivel Mossa y el Ministro Presidente Zaldívar Lelo de Larrea.

afectan las competencias del INAI como órgano garante de los datos personales; 8) no se toman en cuenta los gastos que se van a irrogar al referido Instituto ni tampoco a los concesionarios; y 9) no se dice nada con relación al principio de presunción de inocencia.

- b) Cámara de Senadores. 1) Únicamente se transcribe el dictamen de la colegisladora, centrándose en justificar la necesidad de la reforma sin ningún sustento normativo adicional; 2) tiene un enfoque punitivo pues contempla el combate al delito desde la óptica de la sanción en vez de la implementación de medidas preventivas o complementarias, como pudiera ser la regulación de las tarjetas SIM; 3) es opaco, ya que se convocó a expertos y no se tomaron en cuenta sus conclusiones; y 4) al igual que el de la colegisladora, adolece de la misma falta de justificación de la medida.
60. Conviene recordar que este Tribunal Pleno ya ha referido ampliamente que la garantía de fundamentación y motivación contenida en el artículo 16 constitucional es un derecho de los ciudadanos. A saber, tal artículo tutela el derecho a no sufrir molestias en la persona, familia, domicilio, papeles o posesiones, sino “en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento”.
61. Así, el concepto de “fundamentación” se refiere a la obligación de toda autoridad de expresar específicamente los preceptos en los que se basa su actuar (una vertiente refleja del principio jurídico que establece que una autoridad sólo puede hacer lo que una norma expresamente lo habilite a hacer). Por otro lado, el concepto de “motivación” implica que la autoridad debe expresar las razones concretas que determinan su actuación. De esta suerte, el artículo 16 constitucional establece los parámetros que deben seguir las autoridades en el ejercicio de sus competencias.²⁶
62. Sin embargo, tales obligaciones no son predicables sin más al proceso legislativo, puesto que dicho procedimiento sigue sus propias reglas específicas en las cuales se determina quiénes intervienen, qué etapas se siguen, así como los requisitos para que la decisión sea considerada como válida. Por tanto, el artículo 16 constitucional en lo concerniente a la garantía de fundamentación y motivación tiene una interpretación distinta cuando se predica del proceso legislativo, así lo ha zanjado este Tribunal Pleno en su jurisprudencia.
63. En efecto, se ha sostenido que la fundamentación y motivación de un acto legislativo se satisface cuando el legislador actúa dentro de los límites de las atribuciones que la Constitución correspondiente le confiere (**fundamentación**) y cuando las leyes que emite se refieren a relaciones sociales que reclaman ser jurídicamente reguladas (**motivación**), sin que esto implique que todas y cada una de las disposiciones que integran estos ordenamientos deben ser necesariamente materia de una motivación específica.²⁷ Por tanto, la conveniencia y oportunidad de las razones expresadas en las respectivas iniciativas y dictámenes encuentran a su árbitro natural en el debate parlamentario, no en la sede jurisdiccional.
64. Al respecto, debe decirse que el procedimiento legislativo contiene múltiples garantías políticas para la correcta discusión y deliberación del texto de las respectivas normas aprobadas, modificadas o derogadas. Por tanto, **no es factible que esta Suprema Corte de Justicia evalúe en abstracto las razones políticas** por las cuales se adopta, deroga o modifica una norma, como tampoco erigirse como árbitro de la corrección de sus razones o de los modelos que resulten más eficientes.
65. En las ocasiones que este Alto Tribunal se ha pronunciado sobre opciones regulativas específicas (idoneidad de una medida o medidas alternativas menos lesivas a la empelada) ha sido porque se han empleado mecánicas como el test de proporcionalidad o el test de razonabilidad para evaluar su impacto en un derecho fundamental o principio constitucional específico. En ese sentido, debe decirse que **este Tribunal Constitucional únicamente tiene competencia para juzgar si una norma es o**

²⁶ Registro digital: 238212, Instancia: Segunda Sala, Séptima Época, Materias(s): Común, Fuente: Semanario Judicial de la Federación. Volumen 97-102, Tercera Parte, página 143, Tipo: Jurisprudencia

FUNDAMENTACION Y MOTIVACION. De acuerdo con el artículo 16 de la Constitución Federal, todo acto de autoridad debe estar adecuada y suficientemente fundado y motivado, entendiéndose por lo primero que ha de expresarse con precisión el precepto legal aplicable al caso y, por lo segundo, que también deben señalarse, con precisión, las circunstancias especiales, razones particulares o causas inmediatas que se hayan tenido en consideración para la emisión del acto; siendo necesario, además, que exista adecuación entre los motivos aducidos y las normas aplicables, es decir, que en el caso concreto se configuren las hipótesis normativas.

²⁷ Registro digital: 900226, Instancia: Pleno, Séptima Época, Materias(s): Constitucional, Tesis:226, Fuente: Apéndice 2000. Tomo I, Const., Jurisprudencia SCJN, página 269, Tipo: Jurisprudencia

FUNDAMENTACIÓN Y MOTIVACIÓN DE LOS ACTOS DE AUTORIDAD LEGISLATIVA. Por fundamentación y motivación de un acto legislativo, se debe entender la circunstancia de que el Congreso que expide la ley, constitucionalmente esté facultado para ello, ya que estos requisitos, en tratándose de actos legislativos, se satisfacen cuando aquél actúa dentro de los límites de las atribuciones que la Constitución correspondiente le confiere (fundamentación), y cuando las leyes que emite se refieren a relaciones sociales que reclaman ser jurídicamente reguladas (motivación); sin que esto implique que todas y cada una de las disposiciones que integran estos ordenamientos deben ser necesariamente materia de una motivación específica.

no conforme al texto constitucional, no para evaluar de forma aislada las razones otorgadas por el legislador para actuar determinado sentido, o si debieron tomarse en cuenta determinados estudios o doctrina que se estimen de mayor conveniencia. Ello pertenece al ámbito del debate político y parlamentario, no de la discusión judicial.

66. A partir de este parámetro, debe reconocerse que el decreto objeto de análisis cumple con las obligaciones de fundamentación y motivación de los actos de autoridad legislativa.
67. Esto porque dicho decreto **se encuentra debidamente fundado**, dado que su expedición se inserta en el marco competencial que el artículo 73, fracción XVII, de la Constitución General le confiere al Congreso de la Unión, en tanto le faculta para legislar en materia de tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e internet.²⁸
68. En ese sentido, es claro que la nueva regulación implementada es resultado del ejercicio de esta competencia constitucional, pues a través de ella se crea y regula el PANAUT, un registro de las líneas de telefonía móvil que en principio tiene por objeto coadyuvar con las autoridades de seguridad pública en el combate a la delincuencia, estableciéndose una serie de lineamientos, obligaciones y directrices a cargo de los usuarios de telefonía móvil, de los concesionarios de telecomunicaciones y del Instituto Federal de Telecomunicaciones, lo que permite afirmar que dicha normativa se inserta en el ámbito regulativo de la materia prevista por el referido artículo constitucional.
69. Por su parte, la **motivación del acto legislativo** exige que las normas regulen relaciones sociales que reclamen ser jurídicamente reguladas. En ese sentido, del análisis del proceso legislativo es posible apreciar que la necesidad de introducir esta nueva regulación derivó del crecimiento exponencial de los delitos cometidos a través de dispositivos móviles –principalmente secuestro y extorsión–, lo cual afecta la percepción de seguridad social y bienestar de la población.
70. En consecuencia, el legislador ideó crear una base de datos con la información de los titulares de las líneas de telefonía móvil, a fin de combatir de una manera más eficiente estos delitos mediante un padrón ligado a la titularidad de las líneas de telefonía móvil. En esa tesitura, las razones son claramente formuladas en la exposición de motivos y los correspondientes dictámenes. Por tanto, debe concluirse que el Decreto impugnado se encuentra debidamente motivado en el entendimiento que este Alto Tribunal tiene sobre la “motivación” de los actos legislativos.
71. Cabe precisar que estas mismas consideraciones fueron sostenidas por este Tribunal Pleno al resolver la acción de inconstitucionalidad 110/2020.²⁹
72. Por otro lado, no se deja de apreciar que los legisladores hacen valer una serie de argumentos encaminados a demostrar que los trabajos legislativos **no justificaron de manera suficiente o reforzada** la afectación a los derechos a la privacidad, intimidad y protección de los datos personales, pues no se señaló con claridad por qué se estimaba razonable su restricción, por qué debía privilegiarse la seguridad pública frente a la protección de estos derechos, cuál era el fin constitucionalmente válido perseguido, si la medida resultaba idónea para perseguir dicha finalidad, si la medida era estrictamente necesaria en atención a los mecanismos alternativos que ya existen hoy en día en materia de combate al delito y si dicha afectación resulta proporcional a la luz de los beneficios obtenidos.
73. Sin embargo, este Tribunal Pleno advierte que tales argumentaciones no corresponden a un análisis formal sobre la validez del Decreto impugnado a fin de verificar que se hubieran cumplido las reglas del proceso legislativo, por el contrario, constituyen argumentos de naturaleza sustantiva dirigidas a demostrar que la afectación que producen las normas combatidas en los derechos humanos en juego no es razonable ni encuentra justificación.
74. En esa tesitura, debe reiterarse lo sostenido en párrafos anteriores, dado que no corresponde a esta Suprema Corte de Justicia de la Nación analizar la *conveniencia e idoneidad* de las razones políticas formuladas por el legislador a fin de crear, modificar o derogar determinadas normas; por el contrario,

²⁸ Art. 73.- El Congreso tiene facultad:

(...)

XVII.- Para dictar leyes sobre vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet, postas y correos, y sobre el uso y aprovechamiento de las aguas de jurisdicción federal.

(...)

²⁹ Resuelta el quince de febrero de dos mil veintiuno, por unanimidad de nueve votos de las señoras Ministras y de los señores Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá, Esquivel Mossa apartándose de algunas consideraciones, Franco González Salas salvo algunas consideraciones, Pardo Rebolledo salvo las consideraciones alusivas a la confianza legítima, Piña Hernández separándose de las consideraciones, Laynez Potisek, Pérez Dayán y Presidente Zaldívar Lelo de Larrea separándose de las consideraciones.

este Tribunal Constitucional únicamente tiene competencia para juzgar si dichos preceptos son o no conformes al texto constitucional, lo que entraña un **análisis sustantivo** enfocado en verificar la concordancia del ámbito regulativo de la norma frente al texto, principios y valores constitucionales.

75. En consecuencia, no corresponde a este Alto Tribunal erigirse como un árbitro de la corrección de las razones que llevaron al legislador a conducirse en determinado sentido, **pues ello pertenece al ámbito del debate público y parlamentario, no a la discusión judicial.**
76. No es óbice a estas razones la doctrina que esta Corte ha sostenido sobre la *motivación legislativa reforzada*,³⁰ pues la realidad es que dicha doctrina debe entenderse a la luz de casos específicos y muy excepcionales en los que las razones formuladas por el legislador constituyen elementos indispensables en el análisis de validez del acto combatido,³¹ pero de ninguna manera puede interpretarse como una *habilitación general* para que siempre que exista una limitación a derechos humanos, este Alto Tribunal pueda evaluar las razones políticas que llevaron al legislador a actuar en determinado sentido, pues ha quedado claro que ello está fuera del ámbito de la revisión judicial.
77. Es por estas razones que se concluye que estos argumentos formulados por los accionantes no van a ser abordados en esta parte de la resolución, sino que serán abordados en los siguientes apartados, en el que se analizará desde un punto de vista sustantivo, la regularidad constitucional de las normas impugnadas.

III. Violaciones cometidas al aprobarse el dictamen por las comisiones unidas

78. Sostienen los senadores promoventes que, al interior del Senado, la etapa de dictaminación del proyecto de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión estuvo a cargo de las comisiones unidas de Comunicaciones y Transportes y Estudios Legislativos. En esa tesitura, el día veinticinco de marzo de dos mil veintiuno, ambas comisiones fueron convocadas a fin de analizar, discutir y en su caso aprobar el proyecto de dictamen respectivo.
79. Transcurrida la sesión, se narra que el senador Miguel Ángel Mancera Espinosa solicitó reservar algunos artículos del proyecto, lo cual fue rechazado por la Comisión de Comunicaciones y Transportes por una mayoría de ocho votos en contra y cinco a favor, mientras que en la Comisión de Estudios Legislativo existió un empate a tres votos.
80. A continuación, se ordenó someter a votación de los integrantes de la Comisión de Comunicaciones y Transportes el proyecto de dictamen en sus términos, mientras que la Comisión de Estudios Legislativos no pudo llevar a cabo dicha votación pues de conformidad con el artículo 151 numeral 2 del Reglamento del Senado de la República, se tendría que citar a una reunión posterior dado el

³⁰ Registro digital: 165745, Instancia: Pleno, Novena Época, Materias(s): Constitucional, Tesis: P./J. 120/2009, Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXX, Diciembre de 2009, página 1255, Tipo: Jurisprudencia.

MOTIVACIÓN LEGISLATIVA. CLASES, CONCEPTO Y CARACTERÍSTICAS. Los tribunales constitucionales están llamados a revisar la motivación de ciertos actos y normas provenientes de los Poderes Legislativos. Dicha motivación puede ser de dos tipos: reforzada y ordinaria. La reforzada es una exigencia que se actualiza cuando se emiten ciertos actos o normas en los que puede llegarse a afectar algún derecho fundamental u otro bien relevante desde el punto de vista constitucional, y precisamente por el tipo de valor que queda en juego, es indispensable que el ente que emita el acto o la norma razone su necesidad en la consecución de los fines constitucionalmente legítimos, ponderando específicamente las circunstancias concretas del caso. Tratándose de las reformas legislativas, esta exigencia es desplegada cuando se detecta alguna "categoría sospechosa", es decir, algún acto legislativo en el que se ven involucrados determinados valores constitucionales que eventualmente pueden ponerse en peligro con la implementación de la reforma o adición de que se trate. En estos supuestos se estima que el legislador debió haber llevado un balance cuidadoso entre los elementos que considera como requisitos necesarios para la emisión de una determinada norma o la realización de un acto, y los fines que pretende alcanzar. Además, este tipo de motivación implica el cumplimiento de los siguientes requisitos: a) La existencia de los antecedentes fácticos o circunstancias de hecho que permitan colegir que procedía crear y aplicar las normas correspondientes y, consecuentemente, que está justificado que la autoridad haya actuado en el sentido en el que lo hizo; y, b) La justificación sustantiva, expresa, objetiva y razonable, de los motivos por los que el legislador determinó la emisión del acto legislativo de que se trate. Por otra parte, la motivación ordinaria tiene lugar cuando no se presenta alguna "categoría sospechosa", esto es, cuando el acto o la norma de que se trate no tiene que pasar por una ponderación específica de las circunstancias concretas del caso porque no subyace algún tipo de riesgo de merma de algún derecho fundamental o bien constitucionalmente análogo. Este tipo de actos, por regla general, ameritan un análisis poco estricto por parte de la Suprema Corte, con el fin de no vulnerar la libertad política del legislador. En efecto, en determinados campos -como el económico, el de la organización administrativa del Estado y, en general, en donde no existe la posibilidad de disminuir o excluir algún derecho fundamental- un control muy estricto llevaría al juzgador constitucional a sustituir la función de los legisladores a quienes corresponde analizar si ese tipo de políticas son las mejores o resultan necesarias. La fuerza normativa de los principios democrático y de separación de poderes tiene como consecuencia obvia que los otros órganos del Estado -y entre ellos, el juzgador constitucional- deben respetar la libertad de configuración con que cuentan los Congresos Locales, en el marco de sus atribuciones. Así, si dichas autoridades tienen mayor discrecionalidad en ciertas materias, eso significa que en esos temas las posibilidades de injerencia del juez constitucional son menores y, por ende, la intensidad de su control se ve limitada. Por el contrario, en los asuntos en que el texto constitucional limita la discrecionalidad del Poder Legislativo, la intervención y control del tribunal constitucional debe ser mayor, a fin de respetar el diseño establecido por ella. En esas situaciones, el escrutinio judicial debe entonces ser más estricto, por cuanto el orden constitucional así lo exige. Conforme a lo anterior, la severidad del control judicial se encuentra inversamente relacionada con el grado de libertad de configuración por parte de los autores de la norma.

³¹ Por ejemplo, la creación de un municipio, la ratificación de jueces y magistrados o el establecimiento de cuotas o tarifas de ciertos materiales en los que se brinda la información pública solicitada por el gobernado. Véanse las controversias constitucionales 11/2004, 4/2005 y 32/2007, así como las acciones de inconstitucionalidad 97/2021, 25/2021, 33/2021 y 9/2021.

empate alcanzado sobre la reserva.³² En consecuencia, en dicha sesión el dictamen fue aprobado por la Comisión de Comunicaciones y Transportes por una mayoría de nueve votos por cinco en contra, mientras que la Comisión de Estudios Legislativos lo aprobó hasta la sesión de seis de abril de dos mil veintiuno, por una mayoría de cuatro votos por dos en contra.

81. Señalan los accionantes que tales actuaciones constituyen una violación al artículo 150, numeral 3, del Reglamento del Senado de la República, puesto que conforme a dicho ordenamiento los dictámenes producidos bajo la modalidad de trabajo de comisiones unidas **deben ser aprobados en ese acto por la mayoría absoluta de los integrantes** de cada una de las comisiones que participan, de ahí que no resultaba posible que el dictamen fuera votado primero por la Comisión de Comunicaciones y Transportes, tomando en cuenta que la reserva que estaba pendiente en su homóloga podía influir en el voto del resto de sus integrantes.
82. Este Tribunal Pleno estima que tales argumentos son **infundados**.
83. El artículo 150, numeral 3, del Reglamento del Senado de la República establece lo siguiente:

“Artículo 150

1. Las decisiones en las comisiones se adoptan con el voto de la mayoría absoluta de sus integrantes presentes.

2. Las votaciones sobre dictámenes o resoluciones requieren de la mayoría absoluta de los integrantes de la respectiva comisión.

3. Los dictámenes y resoluciones que se producen bajo la modalidad de trabajo en comisiones unidas, son aprobados por la mayoría absoluta de los integrantes de cada una de las comisiones que participan.

4. Las votaciones nominales se realizan a través del sistema electrónico.”

84. Contrario a lo alegado por los senadores, del texto de la norma no se desprende que cuando se trabaje bajo la modalidad de comisiones unidas, el dictamen tiene necesariamente que aprobarse en un solo acto por ambas comisiones, por el contrario, lo único que se impone es que dicha aprobación debe darse por la mayoría absoluta de los integrantes de cada una de las comisiones que participan, requisito que en el caso se cumplió.³³
85. Esto porque en la Comisión de Comunicaciones y Transportes el dictamen fue aprobado por el voto de nueve de los catorce integrantes, mientras que en la Comisión de Estudios Legislativos se aprobó por cuatro de sus seis integrantes. En consecuencia, no se advierte una vulneración al precepto referido.
86. No resulta óbice a lo anterior que se haya votado y aprobado el dictamen respectivo en la Comisión de Comunicaciones y Transportes mientras estaba pendiente la votación de una reserva en la Comisión de Estudios Legislativos, pues se reitera, no existe una norma que obligue a las comisiones que trabajan bajo la modalidad de *comisiones unidas* a que deban aprobar el dictamen respectivo en el mismo acto o de forma simultánea, por lo que no existía impedimento técnico o jurídico para que las comisiones actuaran en los términos en que lo hicieron, como tampoco se aprecia alguna afectación relevante que trastocara la calidad democrática de la decisión.
87. En consecuencia, dado que son **infundados** los planteamientos formulados por los senadores promoventes lo procedente es reconocer la validez del proceso legislativo que dio lugar al Decreto de reformas de la Ley Federal de Telecomunicaciones y Radiodifusión y emprender el estudio material de las normas combatidas.

³² Artículo 151

1. Cuando en una votación de comisión sobre un asunto se produce empate, se delibera y vota de nuevo en la misma reunión.

2. Si resulta empate por segunda vez, se trata el asunto en una reunión posterior, previo acuerdo de la comisión.

3. Si el empate persiste en la segunda reunión de la comisión, se informa de ello a la Mesa para justificar el retraso en la presentación del dictamen o para los efectos conducentes.

³³ Para efectos de claridad en la votación emitida por el Pleno de la Suprema Corte de Justicia de la Nación en las sesiones de los días veinticinco y veintiséis de abril de dos mil veintidós, específicamente, en relación con el voto emitido por los señores Ministros Aguilar Morales y Gutiérrez Ortiz Mena, quienes, respectivamente, manifestaron apartarse de los párrafos 83 y 85 del proyecto de sentencia sometido a consideración del tribunal Pleno, se informa que, derivado de las modificaciones aceptadas en dichas sesiones, tales párrafos pasaron a ser los números 84 y 86 en el presente engrose.

88. **SÉPTIMO. Vulneración a los derechos de privacidad, intimidad y protección de datos personales**
89. Sobre las cuestiones de fondo, se advierte que los accionantes formulan un gran número de argumentos encaminados a combatir el Decreto por virtud del cual se crea y regula el PANAUT. No obstante, del análisis integral de tales argumentos es posible desprender que **el núcleo de la impugnación** gira en torno a la vulneración de los derechos humanos a la privacidad, intimidad y protección de datos personales, dado que se estima que el PANAUT configura una intromisión injustificada en estos derechos.
90. En esa tesitura, este Tribunal Pleno considera que, metodológicamente, resulta de mayor conveniencia abordar dicho núcleo impugnativo como eje toral en la construcción de la presente resolución, para, a partir de ello, analizar el cúmulo de argumentos que hacen valer los accionantes.
91. Como se señaló, ambos promoventes sostienen que las normas combatidas introducen una afectación injustificada a los derechos humanos a la privacidad, intimidad y protección de datos personales, como consecuencia de la creación y regulación del Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT), el cual impone la obligación a los usuarios de telefonía móvil de entregar a particulares y al Estado sus datos personales e íntimos, tales como nombre, denominación o razón social, nacionalidad, clave única de registro de población, datos biométricos, domicilio, etcétera.
92. Sobre el particular, señalan que la protección de estos derechos no solo implica que las autoridades están obligadas a salvaguardar todos los datos personales e íntimos que tengan en su posesión, sino que también protege un momento previo, esto es, **su recopilación y obtención**, por lo que cualquier acto que pretenda realizar estas conductas debe estar plenamente justificado.
93. En ese sentido, alegan que la normativa impugnada no satisface esta condición, pues autoriza al Estado a recabar datos de manera indiscriminada sin tener una justificación para ello, ya que la finalidad perseguida además de no ser clara y concreta, no resulta adecuada, tomando en cuenta que no existe evidencia que garantice que tener una base de datos con la información personal de los usuarios de telefonía móvil constituya una herramienta útil en el combate a la delincuencia, además de ya existir otras medidas para tales fines que resultan menos restrictivas de los derechos en cuestión.
94. Además, no se justifica por qué debe privilegiarse la seguridad pública frente a la protección de estos derechos.
95. Agregan que la regulación resulta excesiva, puesto que, por un lado, ordena recabar datos de todos los usuarios de telefonía móvil, sin distinción, lo cual incluye a menores de edad con todo lo que ello implica, pero, además, la exigencia versa sobre un espectro demasiado amplio pues recaba información que permite obtener una radiografía completa de la vida de las personas lo cual no puede estar justificado.
96. En esa tesitura, consideran que el PANAUT genera un sistema de vigilancia permanente e indiscriminado que permite al Estado interferir y monitorear directamente la vida privada de las personas, lo cual es abiertamente contrario a los principios que orientan el funcionamiento de una democracia constitucional contemporánea. Ello sin que la medida conlleve beneficios concretos frente a los derechos sacrificados, garantice la certeza en el uso de los datos, ofrezca un mecanismo de rendición de cuentas para quien reclame abusos, ni prevea esquemas que permitan asegurar que los datos extraídos serán debidamente custodiados y empleados sólo con el fin previsto.
97. Además, sostienen que este problema se agrava si se toma en cuenta que, una vez recabada la información, las normas impugnadas no establecen garantías suficientes para la protección de los datos proporcionados, por lo que la privacidad e intimidad de las personas se encuentra totalmente expuesta.
98. Especial mención se hace sobre la intimidad de las personas, pues dentro de los datos que se ordena recabar están los datos biométricos, que se relaciona con los datos más íntimos y sensibles, de ahí que se trata de información radicalmente vedada, por lo que su acceso no solo exige una justificación mucho más estricta, sino que además su protección debe ser reforzada por parte del Estado.
99. En esa medida, ambos accionantes coinciden en sostener que la afectación generada en los derechos fundamentales mencionados no supera una prueba de proporcionalidad.
100. A la luz de tales argumentos, este Tribunal Pleno estima conveniente realizar una segunda precisión metodológica, pues, en función de los planteamientos formulados por los accionantes, es necesario puntualizar que el estudio que se desarrollará a fin de darles respuesta comprenderá **la totalidad de las normas que conforman el Decreto impugnado**.

101. Esto porque de la lectura integral de los conceptos de invalidez se aprecia que los argumentos a partir de los cuales se plantea la vulneración a los derechos a la privacidad, intimidad y protección de datos personales, abarcan **la totalidad de las normas que integran el referido Decreto** en tanto se impugnan como **sistema normativo**.
102. En efecto, la afectación alegada a los derechos humanos en juego se hace derivar directamente de **la creación y regulación** del PANAUT, dado que se estima que la creación de esta base de datos y la forma en la que se encuentra regulada genera una intromisión injustificada y desproporcionada en tales prerrogativas fundamentales. En esa tesitura, la respuesta que debe brindarse sobre si dicha intromisión es o no justificada, abarca necesariamente el sistema normativo que da lugar a dicha base de datos.
103. Realizada esta segunda precisión metodológica, se procede al estudio de los argumentos previamente esbozados.

A) Límites a los derechos humanos y sus condiciones de validez

104. Ha quedado claro entonces que el núcleo de la impugnación de los accionantes versa sobre la intromisión que el PANAUT genera en los derechos humanos a la privacidad, intimidad y protección de datos personales.
105. Al respecto, es conveniente recordar que este Tribunal ha reiterado en diversas ocasiones que los derechos humanos constituyen esferas básicas de protección destinadas a garantizar el reconocimiento y respeto de la dignidad de las personas, de ahí que el artículo 1 constitucional establezca la obligación categórica a cargo de todas las autoridades del Estado de promoverlos, respetarlos, protegerlos y garantizarlos.
106. Sin embargo, también se ha dicho que ningún derecho humano puede plantearse en términos absolutos, pues su interacción en el ordenamiento jurídico conlleva naturalmente la existencia de tensiones o limitaciones, ya sea porque entran en conflicto con otros principios que exigen ser igualmente tutelados, o bien, porque derivado de la relación de interdependencia que existe entre los derechos, la tutela de uno implica o requiere necesariamente la limitación de otro.
107. En consecuencia, este Alto Tribunal ha sido especialmente cuidadoso en señalar que no toda limitación a derechos humanos es en automático inconstitucional o inválida, pues para poder alcanzar dicha conclusión es necesario primeramente analizar si dicha limitante es razonable y justificada a la luz de la metodología que esta Corte ha denominado la *prueba de proporcionalidad*.³⁴
108. Dicha metodología tiene por objeto comprobar, a través del desarrollo de diversos pasos, si efectivamente existe una intromisión en los derechos humanos que se alegan vulnerados y de ser el caso, si dicha intromisión resulta razonable en tanto mantiene un prudente equilibrio entre los valores y principios constitucionales que están en juego. En esa medida, se ha explicado que consta de dos etapas generales.³⁵

³⁴ Registro digital: 160267, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a./J. 2/2012 (9a.), Fuente: Semanario Judicial de la Federación y su Gaceta. Libro V, Febrero de 2012, Tomo 1, página 533, Tipo: Jurisprudencia
RESTRICCIONES A LOS DERECHOS FUNDAMENTALES. ELEMENTOS QUE EL JUEZ CONSTITUCIONAL DEBE TOMAR EN CUENTA PARA CONSIDERARLAS VÁLIDAS. Ningún derecho fundamental es absoluto y en esa medida todos admiten restricciones. Sin embargo, la regulación de dichas restricciones no puede ser arbitraria. Para que las medidas emitidas por el legislador ordinario con el propósito de restringir los derechos fundamentales sean válidas, deben satisfacer al menos los siguientes requisitos: a) ser admisibles dentro del ámbito constitucional, esto es, el legislador ordinario sólo puede restringir o suspender el ejercicio de las garantías individuales con objetivos que puedan enmarcarse dentro de las previsiones de la Carta Magna; b) ser necesarias para asegurar la obtención de los fines que fundamentan la restricción constitucional, es decir, no basta que la restricción sea en términos amplios útil para la obtención de esos objetivos, sino que debe ser la idónea para su realización, lo que significa que el fin buscado por el legislador no se pueda alcanzar razonablemente por otros medios menos restrictivos de derechos fundamentales; y, c) ser proporcional, esto es, la medida legislativa debe respetar una correspondencia entre la importancia del fin buscado por la ley, y los efectos perjudiciales que produce en otros derechos e intereses constitucionales, en el entendido de que la persecución de un objetivo constitucional no puede hacerse a costa de una afectación innecesaria o desmedida a otros bienes y derechos constitucionalmente protegidos. Así, el juzgador debe determinar en cada caso si la restricción legislativa a un derecho fundamental es, en primer lugar, admisible dadas las previsiones constitucionales, en segundo lugar, si es el medio necesario para proteger esos fines o intereses constitucionalmente amparados, al no existir opciones menos restrictivas que permitan alcanzarlos; y en tercer lugar, si la distinción legislativa se encuentra dentro de las opciones de tratamiento que pueden considerarse proporcionales. De igual manera, las restricciones deberán estar en consonancia con la ley, incluidas las normas internacionales de derechos humanos, y ser compatibles con la naturaleza de los derechos amparados por la Constitución, en aras de la consecución de los objetivos legítimos perseguidos, y ser estrictamente necesarias para promover el bienestar general en una sociedad democrática.

³⁵ Registro digital: 2013156, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a. CCLXIII/2016 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 36, Noviembre de 2016, Tomo II, página 915, Tipo: Aislada
TEST DE PROPORCIONALIDAD. METODOLOGÍA PARA ANALIZAR MEDIDAS LEGISLATIVAS QUE INTERVENGAN CON UN DERECHO FUNDAMENTAL. El examen de la constitucionalidad de una medida legislativa debe realizarse a través de un análisis en dos etapas. En una primera etapa, debe determinarse si la norma impugnada incide en el alcance o contenido inicial del derecho en cuestión. Dicho en otros términos, debe establecerse si la medida legislativa impugnada efectivamente limita al derecho fundamental. De esta manera, en esta primera fase corresponde precisar cuáles son las conductas cubiertas prima facie o inicialmente por el derecho. Una vez hecho lo anterior, debe decidirse si la norma impugnada tiene algún efecto sobre dicha conducta; esto es, si incide en el ámbito de protección prima facie del derecho

109. En la primera etapa, debe determinarse si la norma o normas impugnadas inciden o generan un impacto en el alcance o contenido del derecho humano que se estima vulnerado, es decir, debe establecerse si la medida legislativa impugnada limita *prima facie* el derecho fundamental.
110. Para tal efecto, es necesario precisar cuál es el alcance del derecho que se alega comprometido. Una vez hecho lo anterior, debe decidirse si la norma impugnada tiene algún efecto sobre acciones o estados de cosas incluidos de entrada en ese alcance; esto es, si incide en el ámbito de protección *prima facie* del derecho aludido.
111. Si la conclusión es negativa, el examen debe terminar en esta etapa con la declaración de que la medida legislativa impugnada es constitucional al no afectar los derechos que se alegan vulnerados. En cambio, si la conclusión es positiva, debe pasarse al segundo nivel de análisis.
112. En esta segunda fase, para que las intervenciones que se realizan a algún derecho fundamental sean constitucionales debe corroborarse lo siguiente:
- (i) Que la medida legislativa persiga **un fin constitucionalmente válido**. Esta etapa del análisis presupone la idea de que no cualquier propósito puede justificar la limitación a un derecho fundamental. En este orden, los derechos fundamentales, ciertos bienes colectivos y bienes jurídicos garantizados como principios constitucionales, constituyen fines que legítimamente fundamentan la intervención del legislador en el ejercicio de otros derechos.³⁶
 - (ii) Que **la medida resulte idónea** para satisfacer en alguna medida su propósito constitucional. En esta etapa del escrutinio debe analizarse si la medida impugnada tiene, en términos fácticos, una relación de instrumentalidad con el fin, esto es, si es un medio apto para producir el fin perseguido por el legislador. En este sentido, el examen de idoneidad presupone la existencia de una relación entre la intervención al derecho y el fin que persigue dicha afectación, siendo suficiente que la medida contribuya en algún modo y en algún grado a lograr el propósito que busca el legislador.³⁷
 - (iii) Que **la medida resulte necesaria**. El examen de necesidad implica corroborar en términos fácticos, en primer lugar, si existen otros medios igualmente idóneos para lograr los fines que se persiguen y, en segundo lugar, determinar si estas alternativas intervienen con menor

aludido. Si la conclusión es negativa, el examen debe terminar en esta etapa con la declaración de que la medida legislativa impugnada es constitucional. En cambio, si la conclusión es positiva, debe pasarse a otro nivel de análisis. En esta segunda fase, debe examinarse si en el caso concreto existe una justificación constitucional para que la medida legislativa reduzca o limite la extensión de la protección que otorga inicialmente el derecho. Al respecto, es necesario tener presente que los derechos y sus respectivos límites operan como principios, de tal manera que las relaciones entre el derecho y sus límites encierran una colisión que debe resolverse con ayuda de un método específico denominado test de proporcionalidad. En este orden de ideas, para que las intervenciones que se realizan a algún derecho fundamental sean constitucionales debe corroborarse lo siguiente: (i) que la intervención legislativa persiga un fin constitucionalmente válido; (ii) que la medida resulte idónea para satisfacer en alguna medida su propósito constitucional; (iii) que no existan medidas alternativas igualmente idóneas para lograr dicho fin, pero menos lesivas para el derecho fundamental; y, (iv) que el grado de realización del fin perseguido sea mayor al grado de afectación provocado al derecho fundamental por la medida impugnada. En este contexto, si la medida legislativa no supera el test de proporcionalidad, el derecho fundamental preservará su contenido inicial o *prima facie*. En cambio, si la ley que limita al derecho se encuentra justificada a la luz del test de proporcionalidad, el contenido definitivo o resultante del derecho será más reducido que el contenido inicial del mismo.

³⁶ Registro digital: 2013143, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a. CCLXV/2016 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 36, Noviembre de 2016, Tomo II, página 902, Tipo: Aislada

PRIMERA ETAPA DEL TEST DE PROPORCIONALIDAD. IDENTIFICACIÓN DE UNA FINALIDAD CONSTITUCIONALMENTE VÁLIDA. Para que las intervenciones que se realicen a algún derecho fundamental sean constitucionales, éstas deben superar un test de proporcionalidad en sentido amplio. Lo anterior implica que la medida legislativa debe perseguir una finalidad constitucionalmente válida, además de que debe lograr en algún grado la consecución de su fin, y no debe limitar de manera innecesaria y desproporcionada el derecho fundamental en cuestión. Ahora bien, al realizar este escrutinio, debe comenzarse por identificar los fines que persigue el legislador con la medida, para posteriormente estar en posibilidad de determinar si éstos son válidos constitucionalmente. Esta etapa del análisis presupone la idea de que no cualquier propósito puede justificar la limitación a un derecho fundamental. En efecto, los fines que pueden fundamentar la intervención legislativa al ejercicio de los derechos fundamentales tienen muy diversa naturaleza: valores, intereses, bienes o principios que el Estado legítimamente puede perseguir. En este orden de ideas, los derechos fundamentales, los bienes colectivos y los bienes jurídicos garantizados como principios constitucionales, constituyen fines que legítimamente fundamentan la intervención del legislador en el ejercicio de otros derechos.

³⁷ Registro digital: 2013152, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a. CCLXVIII/2016 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 36, Noviembre de 2016, Tomo II, página 911, Tipo: Aislada

SEGUNDA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA IDONEIDAD DE LA MEDIDA LEGISLATIVA. Para que resulten constitucionales las intervenciones que se realicen a un derecho fundamental, éstas deben superar un test de proporcionalidad en sentido amplio. Lo anterior implica que la medida legislativa debe perseguir una finalidad constitucionalmente válida, lograr en algún grado la consecución de su fin y no limitar de manera innecesaria y desproporcionada el derecho fundamental en cuestión. Por lo que hace a la idoneidad de la medida, en esta etapa del escrutinio debe analizarse si la medida impugnada tiende a alcanzar en algún grado los fines perseguidos por el legislador. En este sentido, el examen de idoneidad presupone la existencia de una relación entre la intervención al derecho y el fin que persigue dicha afectación, siendo suficiente que la medida contribuya en algún modo y en algún grado a lograr el propósito que busca el legislador. Finalmente, vale mencionar que la idoneidad de una medida legislativa podría mostrarse a partir de conocimientos científicos o convicciones sociales generalmente aceptadas.

intensidad el derecho fundamental afectado. Así, de encontrarse alguna medida alternativa que sea igualmente idónea para proteger el fin constitucional y que a su vez intervenga con menor intensidad al derecho, deberá concluirse que la medida elegida por el legislador es inconstitucional.³⁸

- (iv) **La proporcionalidad en estricto sentido.** Esta grada de la prueba consiste en efectuar un balance o ponderación entre dos principios que compiten en un caso concreto. Dicho análisis requiere centralmente una valoración, es decir, un juicio axiológico, que consiste en ponderar si la importancia constitucional de lograr el fin perseguido por el legislador es congruente con la importancia de evitar el grado de afectación que se producirá al derecho fundamental. Este juicio valorativo tiene como trasfondo fáctico, naturalmente, el grado de seguridad fáctica respecto de que se logrará ese fin y se producirá esa afectación, respectivamente. En este sentido, mientras más importante sea evitar afectar un derecho fundamental, más importancia debe tener la realización del fin perseguido por el legislador, y más relevancia cobra la certeza de que ese fin se producirá afectando en esa medida el derecho fundamental.³⁹

113. En caso de que la afectación a los derechos humanos alegada supere estas cuatro gradas, entonces deberá concluirse que la norma o normas combatidas son constitucionales, puesto que la afectación a tales derechos es razonable y está justificada. Por el contrario, si dicha afectación no supera alguna de las gradas mencionadas, entonces, deberá concluirse que la norma o normas son inválidas.
114. Ahora bien, debe precisarse que estas gradas corresponden al denominado test *ordinario* de proporcionalidad, aplicable en general a normas que restringen derechos humanos⁴⁰, sin embargo, de forma paralela este Alto Tribunal ha desarrollado un test *estricto*, el cual se exige cuando se combaten distinciones legislativas que se apoyan en una de las denominadas *categorías sospechosas* previstas

³⁸ Registro digital: 2013154, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a. CCLXX/2016 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 36, Noviembre de 2016, Tomo II, página 914, Tipo: Aislada
TERCERA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA NECESIDAD DE LA MEDIDA LEGISLATIVA. Para que resulten constitucionales las intervenciones que se realicen a algún derecho fundamental, éstas deben superar un test de proporcionalidad en sentido amplio. Lo anterior implica que la medida legislativa debe perseguir una finalidad constitucionalmente válida, lograr en algún grado la consecución de su fin y no limitar de manera innecesaria y desproporcionada el derecho fundamental en cuestión. Así, una vez que se ha constatado un fin válido constitucionalmente y la idoneidad de la ley, corresponde analizar si la misma es necesaria o si, por el contrario, existen medidas alternativas que también sean idóneas pero que afecten en menor grado el derecho fundamental. De esta manera, el examen de necesidad implica corroborar, en primer lugar, si existen otros medios igualmente idóneos para lograr los fines que se persiguen y, en segundo lugar, determinar si estas alternativas intervienen con menor intensidad el derecho fundamental afectado. Lo anterior supone hacer un catálogo de medidas alternativas y determinar el grado de idoneidad de éstas, es decir, evaluar su nivel de eficacia, rapidez, probabilidad o afectación material de su objeto. De esta manera, la búsqueda de medios alternativos podría ser interminable y requerir al juez constitucional imaginarse y analizar todas las alternativas posibles. No obstante, dicho escrutinio puede acotarse ponderando aquellas medidas que el legislador consideró adecuadas para situaciones similares, o bien las alternativas que en el derecho comparado se han diseñado para regular el mismo fenómeno. Así, de encontrarse alguna medida alternativa que sea igualmente idónea para proteger el fin constitucional y que a su vez intervenga con menor intensidad al derecho, deberá concluirse que la medida elegida por el legislador es inconstitucional. En caso contrario, deberá pasarse a la cuarta y última etapa del escrutinio: la proporcionalidad en sentido estricto.

³⁹ Registro digital: 2013136, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a. CCLXXII/2016 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 36, Noviembre de 2016, Tomo II, página 894, Tipo: Aislada
CUARTA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA PROPORCIONALIDAD EN SENTIDO ERICTO DE LA MEDIDA LEGISLATIVA. Para que resulten constitucionales las intervenciones que se realicen a algún derecho fundamental, éstas deben superar un test de proporcionalidad en sentido amplio. Lo anterior implica que la medida legislativa debe perseguir una finalidad constitucionalmente válida, lograr en algún grado la consecución de su fin y no limitar de manera innecesaria y desproporcionada el derecho fundamental en cuestión. Así, una vez que se han llevado a cabo las primeras tres gradas del escrutinio, corresponde realizar finalmente un examen de proporcionalidad en sentido estricto. Esta grada del test consiste en efectuar un balance o ponderación entre dos principios que compiten en un caso concreto. Dicho análisis requiere comparar el grado de intervención en el derecho fundamental que supone la medida legislativa examinada, frente al grado de realización del fin perseguido por ésta. En otras palabras, en esta fase del escrutinio es preciso realizar una ponderación entre los beneficios que cabe esperar de una limitación desde la perspectiva de los fines que se persiguen, frente a los costos que necesariamente se producirán desde la perspectiva de los derechos fundamentales afectados. De este modo, la medida impugnada sólo será constitucional si el nivel de realización del fin constitucional que persigue el legislador es mayor al nivel de intervención en el derecho fundamental. En caso contrario, la medida será desproporcionada y, como consecuencia, inconstitucional. En este contexto, resulta evidente que una intervención en un derecho que prohíba totalmente la realización de la conducta amparada por ese derecho, será más intensa que una intervención que se concrete a prohibir o a regular en ciertas condiciones el ejercicio de tal derecho. Así, cabe destacar que desde un análisis de proporcionalidad en estricto sentido, sólo estaría justificado que se limitara severamente el contenido prima facie de un derecho fundamental si también fueran muy graves los daños asociados a su ejercicio.

⁴⁰ La Suprema Corte también suele realizar, también, un test laxo o de mera razonabilidad, en el que el cumplimiento de las gradas es menos intenso y se prodiga una amplia deferencia al criterio del legislador, cuando se trata de políticas públicas que no restringen directamente derechos humanos, como en materia tributaria, económica, etcétera.

en el artículo 1 constitucional, o bien, cuando la norma opera sobre ciertos derechos fundamentales especialmente sensibles que exigen una tutela reforzada, por lo que la medida analizada requiere de una justificación robusta que venza la presunción de inconstitucionalidad que le afecta.⁴¹

115. En estos casos, las gradas que deben analizarse son las siguientes:

- i. Que la medida legislativa persiga **un fin constitucionalmente imperioso**, es decir, debe perseguir un objetivo constitucionalmente importante y no simplemente una finalidad constitucionalmente admisible.
- ii. La medida debe estar **estrechamente vinculada** con la finalidad constitucionalmente imperiosa, es decir, debe estar totalmente encaminada a la consecución de la finalidad, sin que pueda considerarse suficiente que esté potencialmente conectada con tales objetivos.
- iii. Finalmente, la medida debe ser **la menos restrictiva** posible a fin de conseguir la finalidad imperiosa desde el punto de vista constitucional.⁴²

⁴¹ Registro digital: 2012592, Instancia: Pleno, Décima Época, Materias(s): Constitucional, Tesis: P./J. 7/2016 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 34, Septiembre de 2016, Tomo I, página 10, Tipo: Jurisprudencia

INTERÉS SUPERIOR DE LOS MENORES DE EDAD. NECESIDAD DE UN ESCRUTINIO ESTRICTO CUANDO SE AFECTEN SUS INTERESES. El interés superior de los niños, niñas y adolescentes implica que el desarrollo de éstos 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 su vida. Así, todas las autoridades deben asegurar y garantizar que en todos los asuntos, decisiones y políticas públicas en las que se les involucre, todos los niños, niñas y adolescentes tengan el disfrute y goce de todos sus derechos humanos, especialmente de aquellos que permiten su óptimo desarrollo, esto es, los que aseguran la satisfacción de sus necesidades básicas como alimentación, vivienda, salud física y emocional, el vivir en familia con lazos afectivos, la educación y el sano esparcimiento, elementos -todos- esenciales para su desarrollo integral. En ese sentido, el principio del interés superior del menor de edad implica que la protección de sus derechos debe realizarse por parte de las autoridades a través de medidas reforzadas o agravadas en todos los ámbitos que estén relacionados directa o indirectamente con los niños, niñas y adolescentes, ya que sus intereses deben protegerse siempre con una mayor intensidad. En esa lógica, cuando los juzgadores tienen que analizar la constitucionalidad de normas, o bien, aplicarlas, y éstas inciden sobre los derechos de los niños, niñas y adolescentes, es necesario realizar un escrutinio más estricto en relación con la necesidad y proporcionalidad de la medida de modo que se permita vislumbrar los grados de afectación a los intereses de los menores y la forma en que deben armonizarse para que dicha medida sea una herramienta útil para garantizar el bienestar integral del menor en todo momento.

Registro digital: 2016865, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a. XXXIX/2018 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 54, Mayo de 2018, Tomo II, página 1230, Tipo: Aislada

LIBERTAD DE EXPRESIÓN. RESTRICCIONES Y MODALIDADES DE ESCRUTINIO. Dicha libertad es la más asociada a las precondiciones de la democracia constitucional, pues a través de su ejercicio se permite a los ciudadanos discutir y criticar a los titulares del poder público, así como debatir reflexivamente para la formación de posición frente a los problemas colectivos. Sobre tales premisas, las restricciones para el ejercicio de la libertad de expresión deben someterse a distintas intensidades de escrutinio constitucional dependiendo si se proyectan sobre discursos valiosos para esas precondiciones democráticas. Así, pueden identificarse tres tipos de restricciones ligadas a distintas modalidades de escrutinio: 1) restricciones neutrales respecto de los contenidos, que son aquellas que se establecen sin tomar en consideración el tipo de ideas a expresar por las personas; aquí se encuentran las medidas que regulan el tiempo, modo y lugar de los distintos tipos de discurso, y éstas se deben evaluar por regla general con un estándar de escrutinio ordinario o de mera razonabilidad, a menos que se demuestre que tengan un efecto desproporcionado en perjuicio de un punto de vista minoritario, o bien, se compruebe que no existe otra posibilidad real para que las personas difunden los discursos; 2) restricciones dirigidas contra un determinado punto de vista, que son aquellas medidas que singularizan una determinada idea para hacerla merecedora de una restricción o de promoción en el debate público, comúnmente en la forma de un reproche o aprobación oficial; dichas medidas se toman para proteger el lado preferido de un debate y minar aquel lado que se rechaza. La medida busca silenciar un punto de vista y visibilizar otro distinto y 3) restricciones dirigidas a remover un determinado contenido de la discusión, que son aquellas que identifican determinados temas, sin importar el punto de vista o el lado ocupado en el debate, para removerlos de su consideración pública o, bien para consagrarlos como temas obligados. Estas dos categorías, con independencia del tipo de discurso que regulen, se deben sujetar a un escrutinio estricto. Las medidas que buscan restringir un punto de vista y aquellas que buscan remover contenidos de la discusión tienen en común la pretensión de clasificar discursos para inhabilitarlos o bien promoverlos; sin embargo, ambas tienen distintos efectos en la deliberación; así, las primeras buscan influir en el debate, sin impedir la discusión del tema en cuestión, pero sí tomando partido por una de las posiciones, esperando que dicha posición prevalezca, mientras que las segundas son indiferentes a las posiciones de la discusión y buscan más bien remover el tema enteramente de toda consideración o bien posicionarlo en la conversación de manera forzosa. Aunque ambas medidas se deben sujetar a escrutinio estricto, estas últimas suelen arrojar mayor sospecha de inconstitucionalidad, pues a través de ellas el Estado buscar dictar una ortodoxia oficial.

⁴² Registro digital: 2012589, Instancia: Pleno, Décima Época, Materias(s): Constitucional, Tesis: P./J. 10/2016 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 34, Septiembre de 2016, Tomo I, página 8, Tipo: Jurisprudencia

CATEGORÍA SOSPECHOSA. SU ESCRUTINIO. Una vez establecido que la norma hace una distinción basada en una categoría sospechosa -un factor prohibido de discriminación- corresponde realizar un escrutinio estricto de la medida legislativa. El examen de igualdad que debe realizarse en estos casos es diferente al que corresponde a un escrutinio ordinario. Para llevar a cabo el escrutinio estricto, en primer lugar, debe examinarse si la distinción basada en la categoría sospechosa cumple con una finalidad imperiosa desde el punto de vista constitucional, sin que deba exigirse simplemente, como se haría en un escrutinio ordinario, que se persiga una finalidad constitucionalmente admisible, por lo que debe perseguir un objetivo constitucionalmente importante; es decir, proteger un mandato de rango constitucional. En segundo lugar, debe analizarse si la distinción legislativa está estrechamente vinculada con la finalidad constitucionalmente imperiosa. La medida legislativa debe estar directamente conectada con la consecución de los objetivos constitucionales antes señalados; es decir, la medida debe estar totalmente encaminada a la consecución de la finalidad, sin que se considere suficiente que esté potencialmente conectada con tales objetivos. Por último, la distinción legislativa debe ser la medida menos restrictiva posible para conseguir efectivamente la finalidad imperiosa desde el punto de vista constitucional.

Registro digital: 2010595, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a./J. 87/2015 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 25, Diciembre de 2015, Tomo I, página 109, Tipo: Jurisprudencia

CONSTITUCIONALIDAD DE DISTINCIONES LEGISLATIVAS QUE SE APOYAN EN UNA CATEGORÍA SOSPECHOSA. FORMA EN QUE DEBE APLICARSE EL TEST DE ESCRUTINIO ESTRICTO. La constitucionalidad de las distinciones legislativas que se apoyan en una categoría sospechosa debe analizarse a través de un escrutinio estricto, pues para estimarse constitucionales requieren de una justificación robusta que venza la presunción de inconstitucionalidad que las afecta. Para ello, en primer lugar, debe examinarse si la distinción basada en

116. Precisados estos aspectos, corresponde ahora aplicar dicha prueba al caso concreto a fin de poder determinar si el Decreto combatido efectivamente genera una afectación en los derechos fundamentales invocados por los accionantes y de ser el caso, si dicha afectación es razonable y justificada.

B) Análisis de las normas impugnadas a la luz de la prueba de proporcionalidad

I. Primera etapa. Análisis de la afectación *prima facie* de los derechos humanos comprometidos

i) Ámbito de protección de los derechos a la privacidad, intimidad y protección de datos personales.

117. Siguiendo la metodología expuesta, corresponde analizar en primer lugar si el Decreto impugnado tiene un impacto o genera *prima facie* una afectación en los derechos humanos referidos. Para tal efecto, debe examinarse cuál es el alcance de estos derechos.

118. Los derechos a la vida privada y la protección de los datos personales se encuentran reconocidos en los artículos 6 y 16 de la Constitución General, los cuales establecen lo siguiente:

“Art. 6o.- La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

(...)

A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

(...)

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

(...)”

“Art. 16.- Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.

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, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

(...)

119. Por su parte, desde el ámbito internacional, el derecho a la privacidad se encuentra reconocido y protegido en diversas declaraciones y tratados de derechos humanos, tales como la Declaración Universal de los Derechos Humanos (artículo 12),⁴³ el Pacto Internacional de Derechos Civiles y

la categoría sospechosa cumple con una finalidad imperiosa desde el punto de vista constitucional, es decir, debe perseguir un objetivo constitucionalmente importante y no simplemente una finalidad constitucionalmente admisible. En segundo lugar, debe analizarse si la distinción legislativa está estrechamente vinculada con la finalidad constitucionalmente imperiosa, es decir, debe estar totalmente encaminada a la consecución de la finalidad, sin que pueda considerarse suficiente que esté potencialmente conectada con tales objetivos. Finalmente, la distinción legislativa debe ser la medida menos restrictiva para conseguir la finalidad imperiosa desde el punto de vista constitucional.

⁴³ Artículo 12

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

Políticos (artículo 17),⁴⁴ la Convención Americana sobre Derechos Humanos (artículo 11),⁴⁵ la Convención sobre los Derechos del Niño (artículo 16)⁴⁶ y el Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (en adelante “el Convenio 108”).⁴⁷

120. Estos instrumentos son coincidentes en la delimitación de la noción de “*lo privado*”, al establecer que las personas tienen derecho a gozar de un ámbito de proyección de su existencia que debe quedar 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 y el desarrollo de su autonomía y su libertad.⁴⁸
121. De manera específica, la Corte Interamericana de Derechos Humanos ha establecido que la vida privada es un concepto amplio que no es susceptible de definiciones exhaustivas, sino que más bien se trata de un ámbito de protección que comprende, entre otros aspectos, la vida sexual, el derecho a establecer y desarrollar relaciones con otros seres humanos, incluyendo la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás.⁴⁹
122. Ha señalado que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública,⁵⁰ y que comprende entre otras dimensiones, la facultad de tomar libremente decisiones 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 la información personal hacia el público.
123. Ha puntualizado que el artículo 11.2 de la Convención Americana protege al individuo frente a la posible interferencia arbitraria o abusiva del Estado. Sin embargo, eso no significa que el Estado cumpla sus obligaciones convencionales con el solo hecho de abstenerse de realizar tales conductas. Además, 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, 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.⁵¹
124. No obstante, el tribunal interamericano ha precisado también que este derecho, como cualquier otro, no es absoluto, por lo que puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias. Por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática.⁵²

⁴⁴ Artículo 17

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

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

⁴⁵ ARTÍCULO 11. Protección de la Honra y de la Dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

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

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

⁴⁶ Artículo 16

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

2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.

⁴⁷ Artículo 1. Objeto y fin

El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de 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»).

⁴⁸ Por ejemplo, la Asamblea General de las Naciones Unidas lo define como el derecho según el cual nadie debe ser objeto de injerencias arbitrarias o ilícitas en su vida privada, su familia, su domicilio o su correspondencia y el derecho a la protección contra tales injerencias. Véase *Asamblea General de las Naciones Unidas*, resolución 69/166, *El derecho a la privacidad en la era digital*, dieciocho de diciembre de dos mil catorce, p. 10.

⁴⁹ *Caso Rosendo Cantú y otra vs México*, Sentencia de treinta y uno de agosto de dos mil diez, párr. 119 y *Caso Atala Riffo y niñas vs Chile*, Sentencia de veinticuatro de febrero de dos mil doce, párr. 162

En el mismo sentido la Corte Europea de Derechos Humanos, *Caso Beyer v. Alemania*, sentencia de 30 de enero de 2020, párr. 73

⁵⁰ *Caso de las Masacres de Ituango vs Colombia*, Sentencia de primero de julio de dos mil seis, párr. 193 y 194, *Caso Escher y otros vs Brasil*, Sentencia de seis de julio de dos mil nueve, párr. 113 y *Caso Tristán Doroso vs Panamá*, Sentencia de veintisiete de enero de dos mil nueve, párr. 55

⁵¹ *Caso Fontevecchia t D'Amico vs Argentina*. Sentencia de veintinueve de noviembre de dos mil once, párr. 48 y 49

⁵² *Cfr. Caso Tristán Donoso Vs. Panamá*, Sentencia de veintisiete de enero de dos mil nueve, párr. 56 y *Caso Escher y otros Vs. Brasil*, Sentencia de seis de julio dos mil nueve, párr. 116

125. En concordancia con el tribunal interamericano, este Tribunal Pleno ha establecido respecto “*de lo privado*” que sus rasgos característicos se refieren a aquello que no atañe a la vida pública, sino al ámbito reservado frente a la acción y al conocimiento de los demás, a lo que se desea compartir con aquellos que uno elige, a las actividades de las personas en la esfera particular relacionadas con el hogar y la familia, así como a los actos que las personas no desempeñan con el carácter de servidores públicos.⁵³
126. En consecuencia, ha reconocido que el derecho a la privacidad constituye una expresión de la dimensión externa del derecho al libre desarrollo de la personalidad, la cual protege esta “*esfera de privacidad*” del individuo en contra de las incursiones externas que limitan la capacidad para tomar ciertas decisiones a través de las cuales se ejerce la autonomía personal.⁵⁴
127. Se apela al derecho de las personas a mantener fuera del conocimiento de los demás ciertas manifestaciones o dimensiones de su existencia y al correspondiente derecho a que los demás no las invadan sin su consentimiento. Inclusive se ha precisado que esta protección no se limita a un espacio físico, sino que se extiende como un impedimento para *cualquier interferencia* o molestia que pudiera efectuarse, por *cualquier medio*, en un ámbito reservado de la vida personal.⁵⁵

⁵³ Contradicción de Tesis 56/2011. Resuelta por sentencia de treinta de mayo de dos mil trece, por mayoría de siete votos de los Ministros Margarita Beatriz Luna Ramos, José Fernando Franco González Salas, Arturo Zaldívar Lelo de Larrea, Jorge Mario Pardo Rebolledo, Sergio A. Valls Hernández, Olga Sánchez Cordero de García Villegas y Alberto Pérez Dayán. Votaron en contra los Ministros Alfredo Gutiérrez Ortiz Mena, José Ramón Cossío Díaz, Luis María Aguilar Morales y Juan N. Silva Meza.

⁵⁴ Registro digital: 2019357, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a./J. 4/2019 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 63, Febrero de 2019, Tomo I, página 491, Tipo: Jurisprudencia DERECHO AL LIBRE DESARROLLO DE LA PERSONALIDAD. SU DIMENSIÓN EXTERNA E INTERNA. La libertad “indefinida” que es tutelada por el derecho al libre desarrollo de la personalidad complementa las otras libertades más específicas, tales como la libertad de conciencia o la libertad de expresión, puesto que su función es salvaguardar la “esfera personal” que no se encuentra protegida por las libertades más tradicionales y concretas. En este sentido, este derecho es especialmente importante frente a las nuevas amenazas a la libertad individual que se presentan en la actualidad. Ahora bien, la doctrina especializada señala que el libre desarrollo de la personalidad tiene una dimensión externa y una interna. Desde el punto de vista externo, el derecho da cobertura a una genérica “libertad de acción” que permite realizar cualquier actividad que el individuo considere necesaria para el desarrollo de su personalidad. En cambio, desde una perspectiva interna, el derecho protege una “esfera de privacidad” del individuo en contra de las incursiones externas que limitan la capacidad para tomar ciertas decisiones a través de las cuales se ejerce la autonomía personal. Al respecto, si bien en un plano conceptual puede trazarse esta distinción entre los aspectos externos e internos, resulta complicado adscribir los casos de ejercicio de este derecho a una sola de estas dimensiones. Ello es así, porque las acciones que realizan los individuos en el ejercicio de su autonomía personal suponen la decisión de llevar a cabo esa acción, al tiempo que las decisiones sobre aspectos que en principio sólo incumben al individuo normalmente requieren de ciertas acciones para materializarlas. En todo caso, parece que se trata de una cuestión de énfasis. Así, mientras que hay situaciones en las que el aspecto más relevante de la autonomía personal se aprecia en la acción realizada, existen otras situaciones en las que el ejercicio de la autonomía se observa más claramente a través de la decisión adoptada por la persona.

⁵⁵ Registro digital: 169700, Instancia: Segunda Sala, Novena Época, Materias(s): Constitucional, Tesis: 2a. LXIII/2008, Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXVII, Mayo de 2008, página 229, Tipo: Aislada DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Dicho numeral establece, en general, la garantía de seguridad jurídica de todo gobernado a no ser molestado en su persona, familia, papeles o posesiones, sino cuando medie mandato de autoridad competente debidamente fundado y motivado, de lo que deriva la inviolabilidad del domicilio, cuya finalidad primordial es el respeto a un ámbito de la vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, con la limitante que la Constitución Política de los Estados Unidos Mexicanos establece para las autoridades. En un sentido amplio, la referida garantía puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad o la intimidad, de lo cual deriva el reconocimiento en el artículo 16, primer párrafo, constitucional, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida.

Registro digital: 2005525, Instancia: Primera Sala, Décima Época, Materias(s): Constitucional, Tesis: 1a. XLIX/2014 (10a.), Fuente: Gaceta del Semanario Judicial de la Federación. Libro 3, Febrero de 2014, Tomo I, página 641, Tipo: Aislada DERECHO A LA VIDA PRIVADA. ALCANCE DE SU PROTECCIÓN POR EL ESTADO. Al igual que otros derechos fundamentales, el derecho a la vida privada no es absoluto, sino que puede restringirse en la medida en que las injerencias en éste no sean abusivas o arbitrarias. Así, la Corte Interamericana de Derechos Humanos ha sostenido que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias de terceros o de la autoridad pública, y prohíbe ese tipo de injerencias en la vida privada de las personas, enunciando diversos ámbitos de ésta, como la vida privada de sus familias. Ahora bien, el Estado debe adoptar medidas positivas para impedir que la intimidad personal y familiar se vulnere por personas ajenas, pero no puede impedir a quien decide difundir aspectos de su vida privada que lo haga, so pretexto de proteger a la familia, pues en ese caso, ya no se está frente a la difusión de la información por parte de un tercero, que es ajeno a ésta, sino que se estaría limitando el derecho de una persona de divulgar la información que le es propia. En resumen, lo que la Constitución Política de los Estados Unidos Mexicanos y las convenciones internacionales buscan impedir es que terceros difundan información de la vida privada ajena, sin consentimiento del titular; de ahí que si la injerencia en la vida privada de que se duele el tercero perjudicado, consiste en la difusión que hicieron otros miembros de su familia, sobre hechos que conciernen a la vida privada de ellas, y que involucran a éste, como causante de la afectación sufrida por ellas, entonces no puede considerarse que dicha difusión resulte arbitraria o abusiva, puesto que se realizó en ejercicio del legítimo derecho que les asiste de difundir información que les es propia, en la medida en que sea veraz, y que las expresiones utilizadas estén protegidas constitucionalmente, por no ser absolutamente vejatorias, esto es, ofensivas, oprobiosas o impertinentes, según el contexto.

128. Bajo esa lógica, este Alto Tribunal ha sido constante en señalar que la protección efectiva de este derecho provee de las condiciones adecuadas para el despliegue de la individualidad de la persona, su autonomía y libertad.⁵⁶
129. De ahí que a nivel internacional se haya reconocido la vinculación de este derecho con un amplio abanico de otros derechos, como el derecho a una vivienda adecuada;⁵⁷ el derecho a la salud;⁵⁸ el derecho a la igualdad;⁵⁹ los derechos reproductivos; la protección en caso de desalojos forzados;⁶⁰ la inviolabilidad de la correspondencia,⁶¹ de las comunicaciones telefónicas, telegráficas o de otro tipo; los registros en el domicilio; los registros personales y corporales,⁶² o el régimen de recopilación y registro de información personal en computadoras, bancos de datos y otros dispositivos.⁶³
130. Ahora bien, se ha explicado que el derecho a la "vida privada" está destinado a variar, legítima y normalmente, tanto por motivos *internos* al propio concepto como por motivos *externos*.⁶⁴

⁵⁶ Sentencia recaída al amparo directo en revisión 2044/2008, aprobada por la Primera Sala el diecisiete de junio de dos mil nueve por unanimidad de cinco votos; sentencia recaída al amparo directo 6/2009, aprobada por la Primera Sala el siete de octubre de dos mil nueve por unanimidad de cinco votos; sentencia recaída al amparo directo 3/2011, aprobada por la Primera Sala el treinta de enero de dos mil trece por unanimidad de cinco votos; sentencia recaída al amparo directo 4/2011, aprobada por la Primera Sala el treinta de enero de dos mil trece por unanimidad de cinco votos; amparo directo en revisión 402/2007; sentencia recaída al amparo directo 28/2010, aprobada por la Primera Sala el veintitrés de noviembre de dos mil once, por mayoría de cuatro votos.

⁵⁷ Comité de Derechos Económicos, Sociales y Culturales, Observación general N° 4, El derecho a una vivienda adecuada (párrafo 1 del artículo 11 del Pacto).

⁵⁸ Comité de Derechos Económicos, Sociales y Culturales, Observación general N° 4, El derecho a una vivienda adecuada (párrafo 1 del artículo 11 del Pacto).

⁵⁹ Comité de Derechos Humanos, Observación general N° 28, Artículo 3.- La igualdad de derechos entre hombres y mujeres.

⁶⁰ Comité de Derechos Económicos, Sociales y Culturales, Observación general N° 7, El derecho a una vivienda adecuada (párrafo 1 del artículo 11 del Pacto): los desalojos forzados.

⁶¹ Comité de Derechos Humanos, Observación general N° 16, Artículo 17 - Derecho a la intimidad.

⁶² Comité de Derechos Económicos, Sociales y Culturales, Observación general N° 14, El derecho al disfrute del más alto nivel posible de salud (artículo 12).

⁶³ Comité de Derechos Humanos, Observación general N° 16, Artículo 17 - Derecho a la intimidad.

En la misma línea véase la tesis: Registro digital: 165823, Instancia: Primera Sala, Novena Época, Materias(s): Constitucional, Tesis: 1a. CCXIV/2009, Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXX, Diciembre de 2009, página 277, Tipo: Aislada 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 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.

⁶⁴ Registro digital: 165824, Instancia: Primera Sala, Novena Época, Materias(s): Constitucional, Tesis: 1a. CCXIII/2009, Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXX, Diciembre de 2009, página 276, Tipo: Aislada DERECHO A LA VIDA PRIVADA. SU CONTENIDO ES VARIABLE TANTO EN SU DIMENSIÓN INTERNA COMO EXTERNA. El contenido del derecho a la intimidad o vida privada está destinado a variar, legítima y normalmente, tanto por motivos que podemos llamar internos al propio concepto como por motivos externos al mismo. La variabilidad interna de la noción de privacidad alude al hecho de que el comportamiento de sus titulares puede influir en la extensión de su ámbito de protección. No se trata sólo de que el entendimiento de lo privado cambie de una cultura a otra y que haya variado a lo largo de la historia, sino que forma parte del derecho a la privacidad, como lo entendemos ahora, la posibilidad de que sus titulares modulen, de palabra o de hecho, su alcance. Algunas personas comparten con la opinión pública, con los medios de comunicación o con un círculo amplio de personas anónimas, informaciones que para otras se inscriben en el ámbito de lo que preservan del conocimiento ajeno. Aunque una pauta de conducta de este tipo no implica que la persona en cuestión deje de ser titular del derecho a la privacidad, ciertamente disminuye la extensión de lo que de entrada puede considerarse incluido dentro de su ámbito de protección. Por su parte, la variabilidad externa deriva de la existencia de fuentes externas de límites al derecho, y alude a la diferencia normal y esperada entre el contenido *prima facie* de los derechos fundamentales y la protección real que ofrecen en los casos concretos, una vez contrapesados y armonizados con otros derechos e intereses, que pueden apuntar en direcciones distintas e incluso

131. La *variabilidad interna* del derecho a la privacidad alude al hecho de que el comportamiento de los titulares del mismo puede influir en la determinación de su ámbito de protección, lo que significa que forma parte del derecho a la privacidad la posibilidad de que sus titulares modulen, de palabra o de hecho, su alcance. Por ejemplo, algunas personas comparten con la opinión pública, con los medios de comunicación o con un círculo amplio de personas, informaciones que para otras se inscriben en el ámbito de lo que preservan del conocimiento ajeno. Así, aunque una pauta de conducta de este tipo no implica que la persona en cuestión deje de ser titular del derecho a la privacidad, ciertamente disminuye la extensión de lo que de entrada puede considerarse incluido dentro de dicho ámbito de protección.
132. Por su parte, la *variabilidad externa* del derecho a la vida privada deriva de la existencia de límites externos al derecho, alude a la diferencia normal y esperada entre el contenido *prima facie* de los derechos fundamentales y la protección real que ofrecen en casos concretos una vez contrapesados y armonizados con otros derechos e intereses que apunten en direcciones distintas e incluso opuestas a las que derivan de su contenido normativo.
133. Dentro de este ámbito general de protección del derecho a la privacidad, se ha identificado el denominado derecho a la intimidad, el cual se encuentra integrado con los extremos más personales de la vida y del entorno familiar de una persona. Así, el concepto de vida privada comprende a la intimidad como 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 lo radicalmente vedado.⁶⁵
134. Por ejemplo, se ha expresado que la información atinente al origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana constituyen datos sensibles, en tanto pueden afectar la esfera más íntima de su titular, pues su utilización indebida puede dar origen a discriminación o implicar un riesgo para la persona, por lo que cuentan con una protección especial.⁶⁶
135. Ahora bien, es importante señalar que en las modernas sociedades de la información, las potenciales agresiones que la posesión de la información personal organizada representan para la intimidad, tienen una relevancia pública enorme, ya que el derecho a la intimidad, además de tener un aspecto de protección de bienes individuales, tiene una importante función para el desarrollo de sociedades democráticas porque, bien entendido, constituye una condición necesaria para el ejercicio del resto de los derechos humanos.
136. En efecto, se ha reconocido que actualmente nos desarrollamos en un contexto en el que las tecnologías de las comunicaciones globales y las prácticas mediáticas plantean serios y crecientes desafíos para las nociones fundamentales tales como privacidad, protección de datos y reputación, así como para la necesidad crucial de proteger y promover la libertad de expresión y de prensa y el libre flujo de información transfronteriza.⁶⁷

opuestas a las que derivan de su contenido normativo. Así, aunque una pretensión pueda en principio relacionarse con el ámbito generalmente protegido por el derecho, si la misma merece prevalecer en un caso concreto, y en qué grado, dependerá de un balance de razones desarrollado de conformidad con métodos de razonamiento jurídico bien conocidos y masivamente usados en los estados constitucionales contemporáneos. Como han expresado canónicamente los tribunales constitucionales y de derechos humanos del mundo, ningún derecho fundamental es absoluto y puede ser restringido siempre que ello no se haga de manera abusiva, arbitraria o desproporcional.

⁶⁵ Registro digital: 171883, Instancia: Primera Sala, Novena Época, Materias(s): Penal, Tesis: 1a. CXLIX/2007, Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXVI, Julio de 2007, página 272, Tipo: Aislada

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 aquella- 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.

⁶⁶ Acción de inconstitucionalidad 21/2013. Resuelta por sentencia de tres de julio de dos mil catorce, aprobada en este punto por unanimidad de diez votos de los señores Ministros Gutiérrez Ortiz Mena, Cossío Díaz con precisiones en cuanto a las consideraciones, Luna Ramos en contra de las consideraciones, Franco González Salas con precisiones en cuanto a las consideraciones, Zaldívar Lelo de Larrea, Pardo Rebolledo con precisiones en cuanto a las consideraciones, Aguilar Morales con precisiones en cuanto a las consideraciones, Valls Hernández con precisiones en cuanto a las consideraciones, Pérez Dayán y Presidente Silva Meza.

En el mismo sentido el artículo 6 del Convenio 108.

"Artículo 6. Categorías particulares de datos

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. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales."

⁶⁷ "Comentarios preliminares sobre una declaración de principios para la protección de la privacidad y de los datos personales de las Américas", presentados por el doctor David P. Stewart y publicados por el Comité Jurídico Interamericano mediante su informe CJI/doc.382/11

137. La creciente sofisticación de la tecnología de la información digital permite a las entidades privadas, así como a los gobiernos, la posibilidad de recabar, analizar y diseminar mayor cantidad de información personal y más rápidamente que nunca. Por otro lado, los nuevos avances en lo que hace a la investigación y al cuidado médico, a las telecomunicaciones, a los sistemas de transporte avanzados y a las transferencias financieras han incrementado de manera dramática el nivel de información generado por cada individuo, lo que exige el despliegue de acciones y medidas por parte de los Estados a fin de proteger de manera efectiva a las personas.⁶⁸
138. Ante tal contexto, un aspecto primordial en el entendimiento de estos derechos es que han dejado de constituir solamente un mecanismo de defensa de un espacio exclusivo y excluyente, para convertirse también en un **derecho activo de control sobre la información personal, y del uso que se le dé**, la denominada *autodeterminación informativa*.⁶⁹
139. Es precisamente en este ámbito donde se inserta la protección de los datos personales.
140. Al respecto, esta Corte ha sostenido que la protección de datos personales tiene su núcleo en la noción de intimidad y privacidad.⁷⁰
141. La protección de datos personales es una expresión de la *autodeterminación informativa*, referida a la facultad de cada persona para decidir libremente sobre el uso y destino de sus datos personales, teniendo en todo momento derecho a acceder, rectificar, cancelar y oponerse legítimamente a su tratamiento.⁷¹
142. Sobre esta materia, resultan orientadores los *Principios Actualizados sobre la Privacidad y la Protección de los Datos Personales* adoptados por el Comité Jurídico Interamericano,⁷² (*en adelante el CJI*) con el objeto de poder contribuir en los países americanos al desarrollo de un marco vigente para salvaguardar los derechos de la persona a la protección de sus datos personales y a la autodeterminación informativa (*en adelante “los Principios del CJI”*).
143. El objetivo de estos principios es proteger a las personas de la recopilación, el uso, la retención y la divulgación ilícitos o innecesarios de datos personales, proporcionando los **elementos básicos de una protección efectiva**, desplegando su ámbito de aplicación sobre aquellos datos recopilados o administrados por entidades públicas o privadas existentes en cualquier soporte físico o digital.
144. Igualmente, útiles resultan los *“Estándares de Protección de Datos Personales para los Estados Iberoamericanos”*, aprobados por unanimidad en el XV Encuentro Iberoamericano de Protección de Datos, celebrado el veinte de junio de dos mil diecisiete, en Santiago de Chile (*en adelante “Los Estándares Iberoamericanos”*).
145. En ellos se contiene un conjunto de directrices orientadoras que pretenden garantizar el ejercicio y tutela efectivos del derecho a la protección de datos personales, así como facilitar el flujo de estos datos a fin de coadyuvar con el crecimiento económico y social de la región, proporcionando un conjunto de principios y derechos comunes que los Estados miembros puedan adoptar y desarrollar en sus legislaciones nacionales logrando contar con reglas homogéneas en la región.
146. Finalmente, encontramos el ya citado Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, el cual en su artículo 1 establece que su fin es garantizar en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de 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»).

⁶⁸ Idem.

⁶⁹ Amparo en Revisión 884/2018. Resuelto por sentencia de quince de mayo de dos mil diecinueve. Unanimidad de cinco votos de los Ministros Norma Lucía Piña Hernández (Ponente), Luis María Aguilar Morales, Jorge Mario Pardo Rebolledo, Alfredo Gutiérrez Ortiz Mena y Juan Luis González Alcántara Carrancá (Presidente).

⁷⁰ Amparo en Revisión 884/2018. Resuelto por sentencia de quince de mayo de dos mil diecinueve. Unanimidad de cinco votos de los Ministros Norma Lucía Piña Hernández (Ponente), Luis María Aguilar Morales, Jorge Mario Pardo Rebolledo, Alfredo Gutiérrez Ortiz Mena y Juan Luis González Alcántara Carrancá (Presidente).

⁷¹ Acción de inconstitucionalidad 101/2017 y su acumulada. Resuelta por sentencia de siete de mayo de dos mil diecinueve, aprobada en este punto por unanimidad de once votos de los señores Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá, Esquivel Mossa, Franco González Salas, Aguilar Morales, Pardo Rebolledo, Piña Hernández apartándose de las consideraciones, Medina Mora I. apartándose de la mayoría de las consideraciones, Laynez Potisek, Pérez Dayán y Presidente Zaldívar Lelo de Larrea.

⁷² “Principios Actualizados sobre la Privacidad y la Protección de los Datos Personales con anotaciones” adoptados mediante la resolución CJI/RES.266 (XCVIII/21), de nueve de abril de dos mil veintiuno.

147. Ahora bien, estos instrumentos internacionales son coincidentes en definir los datos personales como la información que identifica o puede usarse de manera razonable para identificar a una persona física de forma directa o indirecta, especialmente por referencia a un número de identificación, datos de localización, un identificador en línea o a uno o más factores referidos específicamente a su identidad física, fisiológica, genética, mental, económica, cultural o social. Incluye información expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otro tipo.
148. Igualmente, identifican los datos personales sensibles como esta categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas. Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales o vida sexual, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas o el origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal.
149. Cabe precisar que estos conceptos coinciden con las definiciones incorporadas por la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.⁷³
150. Sobre esta base conceptual, debe decirse que la protección de los datos personales es de importancia fundamental para que una persona pueda disfrutar de su derecho a la vida privada, de ahí que deban establecerse garantías adecuadas a fin de impedir cualquier uso de estos datos que pueda ser incompatible con el debido goce de este derecho. Esta necesidad es aún mayor cuando se trata de la protección de datos personales sometidos a tratamiento automatizado, sobre todo cuando se utilizan con fines policiales. El derecho interno debe garantizar que los datos objeto de tratamiento sean pertinentes y no excesivos en relación con los fines para los que se almacenan; y se conserven en una forma que permita la identificación de los interesados durante un tiempo no superior al necesario para la finalidad para la que se almacenan. También se deben establecer garantías adecuadas de que los datos personales conservados estén protegidos eficazmente contra el uso indebido y el abuso. Estas salvaguardas requieren de una mayor fuerza en lo que respecta a la protección de las categorías especiales de datos más sensibles.⁷⁴
151. Sobre los *Datos Personales Sensibles*, el Principio Nueve del CJI establece lo siguiente:

“Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos.”

⁷³ LGPDPSO

Artículo 3. Para los efectos de la presente Ley se entenderá por:

(...)

IX. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

(...)

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

(...)

LFPDPPP

Artículo 3.- Para los efectos de esta Ley, se entenderá por:

(...)

V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

VI. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

(...)

⁷⁴ Véase Corte Europea de Derecho Humanos, Caso S. y Marper v. Reino Unido, Sentencia de cuatro de diciembre de dos mil ocho, párr. 103.

152. Al respecto, el Comité Jurídico Interamericano señala que estos datos merecen protección especial puesto que, si se manejan o se divulgan de manera indebida, darían lugar a una intrusión profunda en la dignidad personal, el honor de la persona afectada y sus libertades fundamentales, pudiendo desencadenar una discriminación ilícita o arbitraria o causar un riesgo de graves perjuicios para su titular.
153. Es por esto que se indica que, como regla general, los datos personales sensibles no deberían ser tratados⁷⁵, excepto cuando el titular haya otorgado su consentimiento explícito para ello, o cuando sea estrictamente necesario para el ejercicio y cumplimiento de las atribuciones y obligaciones específicas del responsable de datos,⁷⁶ o para dar cumplimiento a un mandato legal, razones de seguridad nacional, seguridad pública, orden público, salud pública, o salvaguarda de derechos y libertades de terceros; lo que claramente impone una fuerte limitación frente al tratamiento de este tipo de información.
154. Por su parte, los estándares iberoamericanos establecen lo siguiente:
- “9. Tratamiento de datos personales de carácter sensible*
- 9.1. Por regla general, el responsable no podrá tratar datos personales sensibles, salvo que se presente cualquiera de los siguientes supuestos:*
- a. Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación.*
- b. Se dé cumplimiento a un mandato legal.*
- c. Se cuente con el consentimiento expreso y por escrito del titular.*
- d. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.*
- 9.2. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles, de conformidad con su derecho interno.”*
155. Ahora bien, de todo lo expuesto hasta este punto es posible afirmar que esta trilogía de derechos de la que hemos hablado, aunque distinguibles y autónomos, se encuentran estrechamente vinculados entre sí, puesto que la interdependencia que existe entre sus respectivos ámbitos de tutela dan lugar a un “*bloque de defensa*” el cual busca proteger al individuo de *cualquier interferencia* o molestia que pudiera efectuarse sobre la esfera de su privacidad –*entendida en sentido lato*–, por *cualquier medio*, ya sea que provengan de particulares o bien, del propio Estado.
156. Dentro de dicho bloque destaca este “*ámbito de lo íntimo*” el cual se relaciona con los aspectos más personales e íntimos del sujeto, que exigen una **protección reforzada**, pues su utilización indebida se traduce en una intromisión grave en la esfera de su titular, en la medida en que puede dar origen a discriminación o conllevar un grave riesgo para su persona. Una de sus manifestaciones, son los datos personales sensibles.
157. Igualmente, debe resaltarse que, siguiendo al Tribunal Interamericano,⁷⁷ esta Corte Suprema ha reconocido que estos derechos han dejado de ser solo un ámbito de defensa de un espacio exclusivo y excluyente, para convertirse ahora en un conjunto de **poderes activos** de conocimiento, acceso y control de la información personal dando lugar a llamada *autodeterminación informativa*, es decir, el poder para determinar quién, qué y con qué motivo puede acceder a nuestros datos personales.⁷⁸
158. En esa tesitura, para este Tribunal Pleno resulta de la mayor importancia precisar que esta autodeterminación informativa se desdobra en dos esferas de protección que, aunque estrechamente vinculadas, deben distinguirse a fin de proteger de manera eficaz dicho ámbito de tutela. Así, la

⁷⁵ De conformidad con este instrumento, el Tratamiento de Datos se define de la siguiente manera: “... se usa en un sentido amplio y abarca toda operación o conjunto de operaciones realizado con Datos Personales, incluyendo, de manera enunciativa más no limitativa, la recopilación, acceso, organización, adaptación, indexación, aprovechamiento, registro, almacenamiento, alteración, recuperación, divulgación o transferencia.”

⁷⁶ De conformidad con este instrumento, el Responsable de los Datos se define de la siguiente manera: “...se refiere a la persona física o jurídica, entidad privada, autoridad pública u otro organismo u organización o servicio que (solo o junto con otros) se encarga del Tratamiento y la protección de los Datos Personales en cuestión. Tales personas determinan el contenido, las finalidades y el uso de los Datos Personales.”

⁷⁷ Caso *Fontevecchia t D’Amico vs Argentina*. Sentencia de veintinueve de noviembre de dos mil once, párr. 48

⁷⁸ A. E. Pérez Luño, *Derechos humanos, estado de derecho y constitución*, Tecnos, 9ª ed (1ª ed. 1984), Madrid. Pp. 356 y ss.

autodeterminación informativa protege a la persona frente a: i) la **recopilación y conservación** de su información privada y datos personales (incluyendo la información relativa a la intimidad y datos sensibles), y ii) el **uso** que se le dé a esta información, lo cual incluye el **acceso** por parte de terceros, sean particulares o el Estado.

159. Desde luego, se reconoce que la recopilación y conservación de esta información normalmente se encamina a un posible acceso posterior por parte de terceros, sin embargo, lo cierto es que aunque estrechamente relacionadas, constituyen dos tipos de afectaciones distintas sobre la privacidad y la autodeterminación informativa, de ahí que cada una de ellas debe justificarse por separado, mediante un examen específico a la luz del objetivo que pretende justificarlas y la razonabilidad sobre la afectación que introducen.⁷⁹
160. Solo a través de la limitación de cada una de estas interferencias podrá evaluarse si su eventual efecto acumulativo, combinado con sólidas salvaguardas, permite reconocer la razonabilidad de dicha interferencia.
161. Bajo estas consideraciones, debe concluirse que la protección de este *bloqueo* se erige como un aspecto fundamental en el desarrollo de sociedades democráticas, dado que dicha esfera proporciona a las personas de las condiciones necesarias para el despliegue de su individualidad, autonomía y libertad, de ahí que figure como un presupuesto necesario para el ejercicio del resto de los derechos humanos.
162. Sin embargo, se reitera lo expuesto en párrafos precedentes, pues actualmente nos desarrollamos en un contexto en el que las tecnologías de las comunicaciones globales y las prácticas mediáticas plantean serios y crecientes desafíos para las nociones fundamentales tales como privacidad, protección de datos y reputación, así como para la necesidad crucial de proteger y promover la libertad de expresión y de prensa y el libre flujo de información transfronteriza.⁸⁰
163. La creciente sofisticación de la tecnología de la información digital permite a las entidades privadas, así como a los gobiernos, la posibilidad de recabar, analizar y diseminar mayor cantidad de información personal y más rápidamente que nunca. Por otro lado, los nuevos avances en lo que hace a la investigación y al cuidado médico, a las telecomunicaciones, a los sistemas de transporte avanzados y a las transferencias financieras han incrementado de manera dramática el nivel de información generado por cada individuo, lo que exige el despliegue de acciones y medidas por parte de los Estados a fin de proteger de manera efectiva a las personas.⁸¹
164. En ese sentido, el relator especial sobre la promoción y protección del derecho a la libertad de opinión y expresión señaló que un rasgo común en el derecho es que, debido a que los derechos a la vida privada y a la libertad de expresión son tan fundamentales para la dignidad humana y la gobernanza democrática, las restricciones deben delimitarse de cerca, establecerse en la ley y aplicarse estrictamente y solo en circunstancias excepcionales. Puntualizó que, en la era digital, proteger esos derechos exige una vigilancia excepcional.⁸²
- ii) *Afectación prima facie de los derechos humanos a la privacidad, intimidad y protección de datos personales.*
165. Delimitado de esta forma el ámbito de protección desplegado por estos derechos, corresponde ahora verificar si el Decreto impugnado a partir de la regulación que impone, genera un impacto en dicho ámbito de tutela.
166. Para ello, es necesario analizar el texto de las normas que integran el referido Decreto, el cual se transcribe a continuación:

“De las Atribuciones del Instituto y de su Composición

Artículo 15. Para el ejercicio de sus atribuciones corresponde al Instituto:

(...)

⁷⁹ Sobre este punto el Alto Comisionado de Naciones Unidas ha sostenido que “...la recopilación y conservación de datos de las comunicaciones equivale a una injerencia en la vida privada, independientemente de si posteriormente se consultan o utilizan esos datos...” Véase Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, “*El derecho a la privacidad en la era digital*”, A/HRC/27/37, treinta de junio de dos mil catorce, párr. 20

⁸⁰ “*Comentarios preliminares sobre una declaración de principios para la protección de la privacidad y de los datos personales de las Américas*”, presentados por el doctor David P. Stewart y publicados por el Comité Jurídico Interamericano mediante su informe CJI/doc.382/11

⁸¹ Idem.

⁸² Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye, A/HRC/29/32, Asamblea General de Naciones Unidas, veintidós de mayo de dos mil quince, párr. 15

XLII Bis. Instalar, operar, regular y mantener el Padrón Nacional de Usuarios de Telefonía Móvil; procurar su buen funcionamiento y el intercambio de información con las autoridades competentes, así como establecer los procedimientos para validar la información que deba incorporarse al mismo conforme a los sistemas informáticos y procedimientos que establezca para tal efecto;

(...)

TÍTULO SÉPTIMO

Del Registro Público de Telecomunicaciones

Artículo 176. El Instituto llevará el Registro Público de Telecomunicaciones, el cual estará integrado por el Registro Público de Concesiones, el Padrón Nacional de Usuarios de Telefonía Móvil y el Sistema Nacional de Información de Infraestructura, de conformidad con lo dispuesto en la presente Ley y las disposiciones aplicables que se emitan.

Capítulo I Bis

Del Padrón Nacional de Usuarios de Telefonía Móvil

Artículo 180 Bis. El Instituto expedirá las disposiciones administrativas de carácter general para la debida operación del Padrón Nacional de Usuarios de Telefonía Móvil, el cual es una base de datos con información de las personas físicas o morales titulares de cada línea telefónica móvil que cuenten con número del Plan Técnico Fundamental de Numeración y cuyo único fin 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.

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

Artículo 180 Ter. El Padrón Nacional de Usuarios de Telefonía Móvil contendrá, sobre cada línea telefónica móvil, la información siguiente:

I. Número de línea telefónica móvil;

II. Fecha y hora de la activación de la línea telefónica móvil adquirida en la tarjeta SIM;

III. Nombre completo o, en su caso, denominación o razón social del usuario;

IV. Nacionalidad;

V. Número de identificación oficial con fotografía o Clave Única de Registro de Población del titular de la línea;

VI. Datos Biométricos del usuario y, en su caso, del representante legal de la persona moral, conforme a las disposiciones administrativas de carácter general que al efecto emita el Instituto;

VII. Domicilio del usuario;

VIII. Datos del concesionario de telecomunicaciones o, en su caso, de los autorizados;

IX. Esquema de contratación de la línea telefónica móvil, ya sea pospago o prepago, y

X. Los avisos que actualicen la información a que se refiere este artículo.

Para efectos de este artículo, se entenderá como tarjeta SIM al dispositivo inteligente desmontable utilizado en los equipos móviles, con objeto de almacenar de forma segura la clave de servicio del suscriptor usada para identificarse ante determinada red.

Artículo 180 Quáter. El registro del número de una línea telefónica móvil en el Padrón Nacional de Usuarios de Telefonía Móvil será obligatorio para el usuario, quien deberá proporcionar identificación oficial, comprobante de domicilio y datos biométricos, para la activación del servicio de la línea telefónica móvil, en términos de lo establecido en la presente Ley y en las disposiciones administrativas de carácter general que al efecto emita el Instituto.

Artículo 180 Quintes (sic). Los concesionarios de telecomunicaciones y, en su caso, los autorizados, deberán recabar e ingresar la información sobre la identidad, datos biométricos y domicilio del usuario, así como proporcionar la información con la cual se integrará el Padrón Nacional de Usuarios de Telefonía Móvil.

Para efectos de lo anterior se utilizarán medios digitales y se permitirán medios remotos, siempre que se garantice la veracidad e integridad de la información, conforme a las disposiciones administrativas de carácter general que emita el Instituto.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, registrarán la información relativa a altas, bajas, y demás movimientos asociados a la línea telefónica móvil, que permitan mantener actualizado el Padrón Nacional de Usuarios de Telefonía Móvil.

Los avisos a que se refiere el artículo 180 Ter, fracción X, de esta Ley se presentarán por los medios y en los plazos que se establezcan en las disposiciones administrativas de carácter general que emita el Instituto, considerando las tecnologías y métodos más modernos y de fácil utilización.

En caso de que el aviso contenga datos equívocos o incongruentes con los asientos que obren en el Padrón Nacional de Usuarios de Telefonía Móvil, el Instituto prevendrá al concesionario de telecomunicaciones o, en su caso, al autorizado que haya presentado el aviso para que realice las aclaraciones respectivas, de conformidad con las disposiciones administrativas aplicables.

El usuario titular del servicio que no reconozca como propio un número de línea telefónica móvil vinculado a su nombre o denominación social, podrá solicitar al Instituto, al concesionario de telefonía o, en su caso, al autorizado, la actualización de la información correspondiente o su baja del Padrón Nacional de Usuarios de Telefonía Móvil de conformidad con lo establecido en las disposiciones administrativas aplicables.

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, el registro del número asociado a dicha persona se mantendrá por un plazo de seis meses.

Artículo 180 Sextus. El Instituto validará y corroborará la información del Padrón Nacional de Usuarios de Telefonía Móvil conforme a los sistemas y procedimientos informáticos que resulten aplicables y, en su caso, podrá solicitar a los concesionarios las aclaraciones pertinentes sobre los datos registrados.

Artículo 180 Septimus. 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.

La información contenida en el Padrón Nacional de Usuarios de Telefonía Móvil a que se refiere el artículo 180 Bis será confidencial y reservada en términos de la Ley General de Transparencia y Acceso a la Información Pública, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Las autoridades de seguridad de procuración y administración de justicia, que conforme a las atribuciones previstas en sus leyes aplicables cuenten con la facultad expresa para requerir al Instituto los datos del Padrón Nacional de Usuarios de Telefonía Móvil, podrán acceder a la información correspondiente de acuerdo con lo establecido en los artículos 189 y 190 de esta Ley y demás disposiciones relativas.

Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

I. Colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes.

Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable.

El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta Ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna;

II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

a) Nombre, denominación o razón social y domicilio del suscriptor;

b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se refiere el artículo 189 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.

Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

III. Entregar los datos conservados a las autoridades a que se refiere el artículo 189 de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables.

Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a entregar la información dentro de un plazo máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente;

IV. Contar con un área responsable disponible las veinticuatro horas del día y los trescientos sesenta y cinco días del año, para atender los requerimientos de información, localización geográfica e intervención de comunicaciones privadas a que se refiere este Título.

Para efectos de lo anterior, los concesionarios deberán notificar a los titulares de las instancias a que se refiere el artículo 189 de esta Ley el nombre del responsable de dichas áreas y sus datos de localización; además deberá tener facultades amplias y suficientes para atender los requerimientos que se formulen al concesionario o al autorizado y adoptar las medidas necesarias. Cualquier cambio del responsable deberá notificarse previamente con una anticipación de veinticuatro horas;

V. Establecer procedimientos expeditos para recibir los reportes de los usuarios del robo o extravío de los equipos o dispositivos terminales móviles y para que el usuario acredite la titularidad de los servicios contratados. Dicho reporte deberá incluir, en su caso, el código de identidad de fabricación del equipo;

VI. Realizar la suspensión del servicio de los equipos o dispositivos terminales móviles reportados como robados o extraviados, a solicitud del titular, y realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil.

Los concesionarios deberán celebrar convenios de colaboración que les permitan intercambiar listas de equipos de comunicación móvil reportados por sus respectivos clientes o usuarios como robados o extraviados, ya sea que los reportes se hagan ante la autoridad competente o ante los propios concesionarios;

VII. Realizar el bloqueo inmediato de líneas de comunicación móvil que funcionen bajo cualquier esquema de contratación reportadas por los titulares o propietarios, utilizando cualquier medio, como robadas o extraviadas, y proceder a realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil; así como, realizar la suspensión inmediata del servicio de telefonía móvil cuando así lo instruya el Instituto para efectos del Padrón Nacional de Usuarios de Telefonía Móvil o la autoridad competente para hacer cesar la comisión de delitos, de conformidad con lo establecido en las disposiciones administrativas y legales aplicables;

Capítulo II Bis

Sanciones en materia del Padrón Nacional de Usuarios de Telefonía Móvil

Artículo 307 Bis. Los concesionarios de telecomunicaciones o, en su caso, los autorizados, incurrirán en relación con el Padrón Nacional de Usuarios de Telefonía Móvil, en las infracciones siguientes:

I. Efectuar extemporáneamente el registro de un número de línea telefónica móvil, excediendo los plazos previstos en las disposiciones administrativas de carácter general;

II. No registrar un número de línea telefónica móvil;

III. No registrar las modificaciones o presentar los avisos que actualicen la información de un registro, a que se refiere el artículo 180 Ter de esta Ley;

IV. Hacer uso indebido de las constancias, documentos y demás medios de identificación, relacionados con el registro de un número de línea telefónica móvil;

V. Alterar, omitir, simular o permitir registros o avisos en forma ilícita, registrar datos falsos, proporcionar información falsa o facilitar información a usuarios o terceros que no tengan derecho, acceder sin autorización a la información del Padrón Nacional de Usuarios de Telefonía Móvil o no denunciar alguna irregularidad teniendo la obligación de hacerlo, y

VI. Hacer uso de la información, documentos o comprobantes del Padrón Nacional de Usuarios de Telefonía Móvil, para obtener un lucro indebido, directamente o por interpósita persona.

Artículo 307 Ter. A quien cometa las infracciones a que se refiere el artículo anterior, se le impondrán las multas siguientes:

I. De 20 a 50 Unidades de Medida y Actualización, a la comprendida en la fracción I;

II. De 500 a 1,000 Unidades de Medida y Actualización, a las referidas en las fracciones II y III;

III. De 2,000 a 4,000 Unidades de Medida y Actualización, a la prevista en la fracción IV;

IV. De 10,000 a 15,000 Unidades de Medida y Actualización, a la señalada en la fracción V, y

V. De dos a tres veces el lucro indebido obtenido para la comprendida en la fracción VI.

Artículo 307 Quáter. La aplicación de las sanciones a que se refiere este Título, se hará considerando las circunstancias en que se cometió la infracción, así como la capacidad económica del infractor. Dichas sanciones no lo liberan del cumplimiento de las obligaciones que establece esta Ley, y se aplicarán sin perjuicio de la responsabilidad administrativa, civil o penal que le resulte.

Artículo 307 Quintus. Para la determinación y cuantificación de las multas a que se refiere este Capítulo se aplicará lo dispuesto en el presente Título.

Transitorios.

Primero. El presente Decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Segundo. El Instituto Federal de Telecomunicaciones realizará las acciones necesarias para que las erogaciones que se generen con motivo de instalar, operar, regular y mantener el Padrón Nacional de Usuarios de Telefonía Móvil, se realicen con cargo a su presupuesto aprobado en el presente ejercicio fiscal y subsecuentes.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados serán responsables de cubrir sus costos de implementación, mantenimiento y operación, incluyendo los de conectividad a los servidores del Padrón Nacional de Usuarios de Telefonía Móvil.

Tercero. El Instituto Federal de Telecomunicaciones, dentro de los ciento ochenta días naturales siguientes a la expedición del presente Decreto, deberá emitir las disposiciones administrativas de carácter general a que se refiere el presente Decreto.

La no emisión de las disposiciones de carácter general en el plazo referido en el párrafo anterior, dará motivo a responsabilidad administrativa para los integrantes del órgano de gobierno del Instituto, de conformidad con lo dispuesto por la Ley General de Responsabilidades Administrativas.

Cuarto. En el caso del registro de líneas telefónicas móviles, en cualquiera de sus modalidades, adquiridas con anterioridad a la entrada en vigor del presente Decreto, los concesionarios de telecomunicaciones y, en su caso, los autorizados, contarán con un plazo de dos años a partir de su publicación para cumplir con las obligaciones de registro a que se refiere el presente Decreto.

El Gobierno Federal, a través de la Secretaría de Comunicaciones y Transportes y el Instituto Federal de Telecomunicaciones, así como los concesionarios de telecomunicaciones y, en su caso, los autorizados, durante el plazo de dos años a que hace referencia el párrafo anterior, deberán realizar una campaña de

información dirigida a sus clientes, con la anticipación que les permita cumplir con su obligación de registrar y actualizar sus datos. Para tal efecto los usuarios deberán presentar ante el concesionario o autorizado de que se trate la tarjeta SIM, así como la documentación fehaciente a que hace referencia el artículo 180 Ter de la Ley Federal de Telecomunicaciones y Radiodifusión o a través de los medios tecnológicos que faciliten a los usuarios el registro. También deberán ser informados de que, en caso de no realizar dicho trámite dentro del plazo señalado, se les cancelará la prestación del servicio relacionado con la línea telefónica móvil de que se trate, sin derecho a reactivación, pago o indemnización alguna.

Transcurrido el plazo señalado para el registro de titulares o propietarios de las líneas telefónicas móviles, el Instituto 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.

Quinto. Los concesionarios de telecomunicaciones y, en su caso, los autorizados, deberán realizar el registro de los nuevos usuarios de telefonía móvil, conforme a lo previsto en el presente Decreto, transcurrido el plazo de 6 meses contados a partir de que el Instituto emita las disposiciones administrativas de carácter general a que se refiere el presente Decreto.

Sexto. El Gobierno Federal, a través de la Secretaría de Comunicaciones y Transportes, la Secretaría de Seguridad y Protección Ciudadana y el Instituto Federal de Telecomunicaciones, así como los concesionarios de telecomunicaciones, deberán realizar campañas y programas informativos a sus clientes o usuarios para incentivar la obligación 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.”

167. Entre los aspectos generales que deben destacarse de la normativa transcrita se encuentra el que su objeto es crear y regular el Padrón Nacional de Usuarios de Telefonía Móvil (en adelante PANAUT), el cual es una base de datos que se integra por información personal e íntima de los titulares de cada línea de telefonía móvil, como nombre completo, denominación o razón social, nacionalidad, número de identificación oficial con fotografía o Clave Única de Registro de Población, datos biométricos, domicilio, entre otros.
168. La finalidad de esta base de datos, declarada por el artículo 180 bis, es contar con una herramienta que sea útil y permita colaborar con las autoridades del Estado en materia de seguridad y justicia en asuntos relacionados con la comisión de ciertos delitos, específicamente a través de la identificación de los usuarios de una determinada línea telefónica móvil.
169. Para tal objetivo, las normas impugnadas prevén como **obligatorio** para los usuarios el registro de su línea de teléfono celular ante los concesionarios de telecomunicaciones, previéndose para tal efecto, un régimen diferenciado dependiendo de si se trata de nuevos usuarios o bien, de usuarios que ya contaban con el servicio.
170. En el primer caso, se establece que los nuevos usuarios estarán obligados a proporcionar sus datos personales e íntimos a fin de que pueda activárseles el servicio de telefonía móvil, para lo cual deberán proporcionar su identificación oficial, comprobante de domicilio y datos biométricos. Por su parte, a los usuarios que ya contaban con una línea de telefonía móvil anterior a la expedición del Decreto, se les otorga un plazo de dos años para realizar el registro de su línea, debiendo proporcionar sus datos personales y biométricos, pues de no hacerlo dicha línea les será cancelada, sin derecho a reactivación.
171. De manera correlativa, se ordena a los concesionarios de telecomunicaciones recabar la información sobre la identidad, datos biométricos y domicilio de los usuarios de telefonía móvil para después ingresarla al PANAUT. Se precisa que la instalación, operación, regulación y mantenimiento de este padrón estará a cargo del Instituto Federal de Telecomunicaciones, el cual deberá expedir las disposiciones administrativas de carácter general para su debida operación.
172. Finalmente, se señala que las autoridades de seguridad de procuración y administración de justicia que cuenten con la facultad expresa para requerir al referido Instituto los datos del PANAUT podrán tener acceso a la información correspondiente.

173. Ante este escenario la pregunta que surge es: ¿esta reglamentación genera un impacto *prima facie* en los derechos a la privacidad, intimidad y protección de datos personales?
174. La respuesta se impone por sí misma, pues si estos derechos se interrelacionan para generar una especie de *bloque* que busca proteger la esfera privada del sujeto y mantenerla alejada del escrutinio público, es claro que dicho ámbito se ve afectado al imponer a los usuarios de telefonía móvil la obligación de entregar su información privada, íntima y datos personales, incluyendo datos sensibles, con la correlativa facultad otorgada a terceros particulares y al propio Estado para recopilarlos y poder acceder a ellos.⁸³
175. En ese sentido, la repercusión en estos derechos también debe reconocerse desde su vertiente activa, esto es, en relación con la *autodeterminación informativa*, pues si desde esta perspectiva la persona tiene el poder para determinar quién, qué y con qué motivo puede acceder a sus datos personales, es claro que esta dimensión también se ve impactada por el sistema normativo que crea y regula el PANAUT.
176. Esto porque en virtud de las normas transcritas se crea una base de datos integrada por la información y datos privados de los usuarios de telefonía móvil.
177. Sobre el particular, debe advertirse que la entrega de sus datos personales y sensibles **se impone como una obligación** al usuario de telefonía móvil, lo que significa que para efectos de dicha entrega el consentimiento del usuario no es un elemento relevante, dado que no resulta optativo para él proporcionar o no la información que le es requerida, sino más bien se le impone como una **condición obligatoria** a fin de poder *adquirir o conservar* el servicio de telefonía móvil.
178. Además, el consentimiento del usuario tampoco interviene en el uso y destino que se le dará a su información, ni tampoco sobre quién podrá acceder a ella, pues estos aspectos ya vienen predeterminados por la norma, en tanto se establece que la base de datos que integra el PANAUT servirá para coadyuvar en el combate a la delincuencia, de tal suerte que será recopilada por los concesionarios de las telecomunicaciones, será administrada por el Instituto Federal de Telecomunicaciones y podrá ser consultada por las autoridades de procuración y administración de justicia con el objeto de satisfacer tales finalidades.
179. En consecuencia, es claro que estos elementos impactan directamente en la *autodeterminación informativa* del sujeto, pues a través de las normas combatidas se crea una base de datos integrada por la información privada y personal de los usuarios de telefonía móvil, donde, además, el consentimiento no juega un papel relevante en la entrega, manejo, uso y destino de dicha información. En ese sentido, distinguiendo entre la **recopilación** de la información privada y su **uso**, debe reconocerse que la reglamentación analizada impacta sobre ambos aspectos.
180. De manera adicional, este Tribunal Pleno considera que la intromisión que genera el PANAUT en los derechos a la privacidad, intimidad y protección de datos personales **es intensa** y para justificar esta conclusión, resulta importante tener en cuenta cuatro aspectos que derivan de la reglamentación cuestionada.
181. El primero, el tipo de información que se recaba, pues como puede apreciarse, las normas controvertidas imponen la obligación a los usuarios de telefonía móvil de proporcionar datos como su nombre completo, nacionalidad, número de identificación oficial o Clave Única de Registro de Población, domicilio y datos biométricos, **información que en su conjunto permite extraer conclusiones muy precisas sobre la vida privada de las personas**, permitiendo incluso la determinación de sus perfiles, de ahí que puede generarse en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante. Así, las características propias de este tipo de información exigen una protección reforzada a fin de evitar dejar en un grave estado de vulnerabilidad a la persona, comprometiendo la esfera más básica de su individualidad.
182. Segundo, porque dicha información se entrega directamente al Estado. En efecto, de conformidad con la normativa impugnada, **toda la información recopilada de los usuarios de telefonía móvil pasará en automático a estar en posesión del Estado**, pues se establece que una vez que los concesionarios hayan recabado dicha información deberán ingresarla al PANAUT, el cual va a ser **administrado y operado por el Estado** a través del Instituto Federal de Telecomunicaciones.

⁸³ En ese sentido se pronunció la Corte Europea de Derechos Humanos en el Caso Breyer v. Alemania, sentencia de 30 de enero de 2020, párr. 81.

En el mismo sentido el Tribunal de Justicia de la Unión Europea, véanse los casos Digital Rights Ireland Ltd v. Minister for Communications and others, Asunto C-293/12 y C-594/12, sentencia de ocho de abril de dos mil catorce, párr. 25 a 29; y Tele2 Sverige AB y otros, C 203/15 y C-698/15, sentencia de veintiuno de diciembre de dos mil dieciséis, párr. 98 a 100.

183. Este aspecto, desde luego, contribuye y refuerza esta percepción de las personas afectadas acerca de que su vida privada es objeto de una vigilancia constante. De ahí la necesidad del establecimiento de salvaguardas importantes que eviten la arbitrariedad y el abuso en el acceso y uso de esta información.
184. Por supuesto, no pasa inadvertido que el artículo 180 Septimus establece que las autoridades de seguridad de procuración y administración de justicia, que conforme a las atribuciones previstas en sus leyes aplicables cuenten con la facultad expresa para requerir al Instituto los datos del PANAUT, podrán acceder a la información correspondiente.
185. Sin embargo, debe reconocerse que esta disposición **no regula el acceso del Estado a la información brindada por los usuarios de telefonía móvil**, pues como se señaló, dicha posesión ya la tiene al ser el administrador y operador del PANAUT, de tal suerte que lo que regula el referido precepto **es la transferencia de estos datos** de un órgano del Estado hacia otro, del Instituto Federal de Telecomunicaciones hacia las autoridades de procuración y administración de justicia. Lo cual constituye una diferencia muy importante para efectos de la identificación de la afectación que la regulación reclamada produce en los derechos humanos en juego.
186. En ese sentido, si bien ha quedado establecido que debe distinguirse entre la recopilación y conservación de la información privada de la persona –en sentido lato– y el uso y acceso de dicha información por parte de terceros, lo cierto es que, en el caso concreto, dada la reglamentación específica que establece el Decreto controvertido, en el PANAUT la recopilación y conservación de la información traen por sí mismas el acceso a ella por parte del Estado. De ahí que en los siguientes apartados, aunque se parte de la identificación y distinción entre ambos tipos de afectaciones, lo cierto es que su estudio estará estrechamente vinculado.
187. Tercero, porque la obligación de entregar estos datos personales abarca a todas las personas, físicas o morales, que sean titulares de una línea de telefonía móvil.
188. A fin de dimensionar este aspecto, debe decirse que conforme al Banco de Información de Telecomunicaciones (BIT)⁸⁴ emitido por el Instituto Federal de Telecomunicaciones, al primer trimestre de dos mil veintiuno, el número de líneas telefónicas móviles existentes era de 123,377,078 (ciento veintitrés millones trescientos setenta y siete setenta y ocho), lo que implica que hasta el año pasado existían noventa y ocho líneas por cada cien habitantes.
189. Esto significa que, dada la densidad de líneas de telefonía móvil que existen en el país, el Estado, a partir de la creación y regulación del PANAUT, podrá recopilar, administrar, conservar y tener acceso a la información básica, privada y más íntima de casi toda la población del país, lo que refuerza esta percepción acerca del establecimiento de un sistema generalizado de vigilancia por parte del Estado.
190. Cuarto, la temporalidad, pues del análisis del Decreto combatido no se advierte la existencia de algún precepto que establezca el tiempo por el cual el Estado podrá conservar la información privada de los usuarios, lo que permite inferir entonces, que dicha conservación se realizará por tiempo indefinido, es decir, la afectación a los derechos fundamentales de los usuarios tendrá un carácter permanente.
191. Así, derivado de la valoración conjunta de estos cuatro elementos es posible concluir que el Decreto impugnado no solo genera una afectación *prima facie* en los derechos a la privacidad, intimidad y protección de datos personales, sino que además, dicha injerencia **es fuerte**, pues, a partir del registro de los titulares de cada línea de telefonía móvil en el país, se crea una base de datos con la información privada e íntima de casi toda la población, la cual será administrada y operada por el Estado de manera permanente, condiciones que colocan a los derechos fundamentales en juego en una grave situación de riesgo.
192. Lo anterior implica que el Decreto impugnado satisface la primera etapa de la prueba de proporcionalidad, pues ha quedado demostrado que su ámbito regulativo impacta *fuertemente* en la esfera de protección garantizada por los derechos a la privacidad, intimidad y protección de datos personales.
193. Sentada esta conclusión, y de conformidad con la metodología definida en la presente resolución, lo procedente es pasar a la segunda etapa, es decir, analizar si esta afectación *prima facie* en los derechos fundamentales es razonable a la luz de las distintas gradas que integran el referido test.

⁸⁴ Consultable en el siguiente enlace: <https://bit.ift.org.mx/BitWebApp/informacionEstadistica.xhtml>

194. Sin embargo, antes de proceder a dicho análisis, este Tribunal Pleno considera de gran utilidad referir lo expuesto por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos en su informe anual denominado *"El derecho a la privacidad en la era digital."*⁸⁵ Esto porque en dicho documento se esbozan una serie de parámetros y lineamientos que configuran un preámbulo idóneo del estudio que se desarrollará en los siguientes apartados.
195. En efecto, en el referido informe se explica que, en la era digital, las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos.
196. Los avances tecnológicos han significado que la eficacia de la vigilancia realizada por el Estado ya no se ve limitada por su magnitud o duración. La disminución de los costos de tecnología y almacenamiento de datos ha eliminado los inconvenientes financieros o prácticos de la vigilancia. El Estado no había tenido nunca la capacidad de que dispone actualmente para realizar actividades de vigilancia simultáneas, invasivas, con objetivos precisos y a gran escala. Es decir, las plataformas tecnológicas de las que depende crecientemente la vida política, económica y social a nivel mundial no solo son vulnerables a la vigilancia en masa, sino que en realidad pueden facilitarla.
197. Los ejemplos de actividades de vigilancia digital declaradas y encubiertas en jurisdicciones de todo el mundo se han multiplicado y la vigilancia en masa por parte de los gobiernos se ha revelado como un hábito peligroso y no como una medida excepcional.
198. Por tanto, se reconoció que **toda captura de datos de las comunicaciones es potencialmente una injerencia en la vida privada**, precisándose incluso que la recopilación y conservación de datos de las comunicaciones equivale a una injerencia en la vida privada, independientemente de si posteriormente se consultan o utilizan esos datos. Incluso la mera posibilidad de que pueda captarse información de las comunicaciones crea una injerencia en la vida privada y puede tener un efecto negativo en derechos como los relativos a la libertad de expresión y de asociación. La mera existencia de un programa de vigilancia en masa crea, por lo tanto, una injerencia en la privacidad. **Incumbiría al Estado demostrar que tal injerencia no es arbitraria ni ilegal.**
199. Inclusive, se puntualizó que la vigilancia en masa, la interceptación de las comunicaciones digitales y la recopilación de datos personales, son susceptibles de afectar no solo el derecho a la privacidad de las personas, sino también otros derechos como, por ejemplo, el derecho a la libertad de opinión y de expresión, a buscar, recibir y difundir información; el derecho a la libertad de reunión y de asociación pacíficas; y el derecho a la vida familiar. Todos esos derechos están estrechamente vinculados con el derecho a la privacidad y cada vez más se ejercen a través de los medios digitales.
200. Es por esta razón que se considera que toda limitación a los derechos a la privacidad debe estar prevista en la ley, la cual debe ser lo suficientemente accesible, clara y precisa para que una persona pueda leerla y saber quién está autorizado a realizar actividades de vigilancia de datos y en qué circunstancias. Además, la limitación debe ser necesaria para alcanzar un objetivo legítimo, así como proporcional al objetivo y la opción menos perturbadora de las disponibles. Uno de los factores que deben considerarse al determinar la proporcionalidad es qué se hace con los datos a granel y quién pueden acceder a ellos una vez recopilados.
201. Explicó que debe demostrarse que la limitación impuesta al derecho (una injerencia en la vida privada, por ejemplo, con el fin de proteger la seguridad nacional o el derecho a la vida de otras personas) tiene posibilidades de alcanzar ese objetivo. Por tanto, es responsabilidad de las autoridades que deseen limitar el derecho demostrar que la limitación está relacionada con un objetivo legítimo. Además, las limitaciones al derecho a la privacidad no deben vaciar el derecho de su esencia y deben ser compatibles con otras normas de derechos humanos, incluida la prohibición de la discriminación. Si la limitación no cumple esos criterios, es ilegal y/o la injerencia en el derecho a la privacidad es arbitraria.
202. Así pues, los programas de vigilancia en masa o "a granel" pueden considerarse arbitrarios, aunque persigan un objetivo legítimo y hayan sido aprobados sobre la base de un régimen jurídico accesible. En otras palabras, no es suficiente que las medidas tengan por objeto encontrar determinadas agujas en un pajar; lo importante es el impacto de las medidas en el pajar en comparación con el riesgo de que se trate; es decir, si la medida es necesaria y proporcionada.

⁸⁵ Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *"El derecho a la privacidad en la era digital"*, A/HRC/27/37, 30 de junio de 2014.

203. En esa misma línea de razonamiento, la Corte Europea de Derechos Humanos señaló que la protección de los datos personales es de importancia fundamental para que una persona disfrute de su derecho al respeto de la vida privada y familiar garantizado por el artículo 8 del Convenio Europeo de Derechos Humanos. En ese sentido, estableció que el derecho interno debe ofrecer garantías adecuadas para impedir cualquier uso de los datos personales que pueda ser incompatible con las garantías del referido artículo.
204. Preciso que la necesidad de tales garantías es aún mayor cuando se trata de la protección de datos personales sometidos a tratamiento, sobre todo cuando se utilizan con fines policiales. El derecho interno debe garantizar, en particular, que dichos datos sean pertinentes y no excesivos en relación con los fines para los que se almacenan; y se conserven en una forma que permita la identificación de los interesados durante un tiempo no superior al necesario para la finalidad para la que se almacenan.
205. El derecho interno también debe ofrecer garantías adecuadas de que los datos personales conservados estén protegidos eficazmente contra el uso indebido y el abuso, consideraciones que son especialmente válidas en lo que respecta a la protección de las categorías especiales de datos más sensibles.⁸⁶
206. Al respecto, el Alto Comisionado se refirió a las dudas que plantea la creciente colaboración de los gobiernos con entidades del sector privado a fin de conservar datos “*por si acaso*” los necesita el gobierno. Manifestó que la conservación obligatoria de datos de terceros —característica frecuente de los regímenes de vigilancia de muchos Estados, cuyos gobiernos exigen a las compañías telefónicas y a los proveedores de servicios de internet que almacenen los metadatos acerca de las comunicaciones y la ubicación de sus clientes para que las fuerzas del orden y los organismos de inteligencia puedan acceder posteriormente a ellos— no parece necesaria ni proporcionada.
207. De ahí que, con posterioridad, el relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión señalara que los Estados deben abstenerse de establecer la identificación de usuarios como condición para acceder a las comunicaciones digitales y a los servicios en línea, y de obligar a los usuarios de teléfonos móviles a registrar su tarjeta SIM.
208. Esto porque el registro obligatorio de las tarjetas SIM puede proporcionar a los gobiernos capacidad de vigilar a personas y periodistas más allá de cualquier interés legítimo. Así, la capacidad de un Estado para exigir a los proveedores de servicios de telecomunicaciones y de Internet que recopilen y almacenen información sobre las actividades en línea de todos los usuarios ha resultado de forma inevitable en que el Estado tenga la huella digital de todos los usuarios. La capacidad del Estado para recopilar y almacenar datos personales amplía su capacidad para llevar a cabo labores de vigilancia e incrementa la probabilidad de que se robe y difunda la información personal.⁸⁷
209. Sobre este punto, resulta conveniente remarcar que en su informe “*el derecho a la privacidad en la era digital*” el Alto Comisionado se refirió al papel que juegan las empresas en la protección de la privacidad de las personas, pues reconoció que los gobiernos recurren cada vez más al sector privado para realizar y facilitar las actividades de vigilancia digital, inclusive señaló que ese proceso es cada vez más formalizado pues el traslado de la prestación del servicio de telecomunicaciones del sector público al sector privado ha producido una delegación de las responsabilidades policiales y cuasijudiciales a los intermediarios de internet disfrazada de “autorregulación” o “cooperación”. Así, expresó que la promulgación de leyes que obligan a las empresas a preparar sus redes para la interceptación es motivo de especial preocupación, en particular porque crea un ambiente que facilita las medidas de vigilancia exhaustiva.
210. Expuso que un Estado puede tener motivos legítimos para exigir a una empresa de tecnología de la información y las comunicaciones que le proporcione datos de sus usuarios; sin embargo, cuando una empresa suministra datos o información de sus usuarios a un Estado en respuesta a una solicitud que contraviene el derecho a la privacidad establecido en el derecho internacional, proporciona tecnología o equipos de vigilancia en masa a un Estado sin salvaguardias adecuadas o cuando se da a dicha información otro uso contrario a los derechos humanos, **la empresa en cuestión puede ser cómplice o estar involucrada de otra manera en violaciones de los derechos humanos.**

⁸⁶ Corte Europea de Derechos Humanos, caso *S. and Marper v. The United Kingdom*, sentencia de cuatro de diciembre de dos mil ocho, párr. 103 y 104.

⁸⁷ Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Asamblea General de las Naciones Unidas, A/HRC/29/32, 22 de mayo de 2015, parr. 51, 55 y 60.

211. Es por ello que señaló que cuando los gobiernos exigen a las empresas que les proporcionen acceso a los datos en contravención de las normas internacionales de derechos humanos, las empresas deben tratar de honrar los principios de derechos humanos en la medida de lo posible, y ser capaces de demostrar sus iniciativas en curso para hacerlo. Ello puede entrañar interpretar las demandas del gobierno de la manera más restringida posible, pedir aclaraciones a un gobierno en relación con el alcance y el fundamento jurídico de la demanda, requerir una orden judicial antes de acceder a las peticiones de datos del gobierno, y comunicar de forma transparente a sus usuarios los riesgos y la aceptación de las demandas del gobierno.
212. Expuesto este preámbulo, debe procederse al análisis de la segunda etapa de la prueba de proporcionalidad, en la cual –cabe precisar– se retomarán y desarrollarán estos parámetros o lineamientos generales que han quedado esbozados en los párrafos precedentes.

II. Segunda etapa. Análisis de las distintas gradas que integran la prueba de proporcionalidad

213. Antes de poder entrar a este análisis específico, primero es importante precisar qué tipo de escrutinio corresponde realizar sobre el Decreto impugnado, ya que este aspecto es sumamente relevante en términos del parámetro a partir del cual habrá de medirse la validez constitucional de las normas reclamadas.
214. Ha quedado expuesto que este Tribunal Pleno ha desarrollado tres tipos de escrutinios para analizar la validez constitucional de normas generales: laxo o de mera razonabilidad, ordinario y estricto. El primero aplica a normas que no restringen directamente derechos humanos y se refieren centralmente a políticas públicas y bienes colectivos (fiscales, económicos, etcétera). El segundo, como su nombre lo indica, se aplica en general ante cualquier tipo de limitación a derechos fundamentales. Y el tercero, el *test de escrutinio estricto* es exigible en dos supuestos generales: *i)* cuando se combaten distinciones legislativas que se apoyan en una de las denominadas categorías sospechosas previstas en el artículo 1 constitucional; o *ii)* cuando la norma opera sobre derechos fundamentales *especialmente sensibles* que dadas sus condiciones o importancia en determinados supuestos, exigen una tutela reforzada, de tal suerte que con este escrutinio se busca garantizar que la medida analizada tenga una justificación robusta que derrote la presunción de inconstitucionalidad que pesa sobre ella.
215. En tales condiciones, este Tribunal Pleno advierte que para analizar la validez del Decreto impugnado será necesario aplicar tanto un escrutinio ordinario como uno estricto, tal y como se explicará a continuación.⁸⁸
216. Ha quedado establecido que la creación y regulación del PANAUT impacta *prima facie* en los derechos humanos a la vida privada, intimidad y protección de sus datos personales. Sin embargo, para efectos del parámetro de regularidad, es importante distinguir entre la afectación que sufren los derechos a la privacidad y protección de datos personales, de la afectación que sufren los derechos a la intimidad y protección de los datos sensibles.
217. Lo anterior porque tal y como se explicó en líneas precedentes, la intimidad constituyen un **núcleo protegido con mayor celo y fuerza**, pues dada su estrecha vinculación con los aspectos más íntimos de la persona, exige una protección especial y reforzada, puesto que su conocimiento por parte de terceros coloca a su titular en una situación de extrema vulnerabilidad, al hacerlo objeto de conductas discriminatorias susceptibles de ocasionar graves perjuicios en su esfera y poniendo en riesgo los valores más importantes de su individualidad.
218. Es por esto que las potenciales agresiones a la intimidad han sido reconocidas como de una enorme relevancia no solo desde el punto de vista individual, sino también colectivo, pues este ámbito dota de las condiciones adecuadas para que las personas pueda desplegar adecuadamente su individualidad, autonomía y libertad, de ahí que su protección tenga una importante función para el desarrollo de sociedades democráticas, en tanto se erige como presupuesto indispensable para el ejercicio del resto de los derechos humanos.

⁸⁸ Para efectos de claridad en la votación emitida por el Pleno de la Suprema Corte de Justicia de la Nación en las sesiones de los días veinticinco y veintiséis de abril de dos mil veintidós, específicamente, en relación con el voto emitido por la señora Ministra Ortiz Ahlf, quien manifestó apartarse del párrafo 195 del proyecto de sentencia sometido a consideración del tribunal Pleno, se informa que, derivado de las modificaciones aceptadas en dichas sesiones, dicho párrafo pasó a ser el 215 en el presente engrose.

219. Por lo tanto, dada la especial protección que exige este ámbito, se llega a la conclusión de que las intromisiones a la intimidad y la protección de datos sensibles deben ser analizadas a la luz de un escrutinio estricto,⁸⁹ mientras que las injerencias al derecho a la privacidad y la protección de los datos personales en general deben ser revisadas a la luz de un escrutinio ordinario.
220. En consecuencia, en los siguientes apartados de la presente resolución se deberá responder a estas dos preguntas:
- a) ¿El sistema normativo que permite al Estado a través del PANAUT recopilar, administrar, conservar por tiempo indeterminado y tener acceso a la **información privada y los datos personales** de toda aquella persona física y/o moral que sea titular de una línea telefónica (i) persigue una finalidad constitucionalmente válida; (ii) es idóneo para la consecución de dicha finalidad; (iii) constituye una medida necesaria; y (iv) es proporcional en sentido estricto? (Test ordinario).
 - b) ¿El sistema normativo que permite al Estado a través del PANAUT recopilar, administrar, conservar por tiempo indeterminado y tener acceso a la **información íntima y los datos personales sensibles** de toda aquella persona física y/o moral que sea titular de una línea telefónica (i) persigue un fin constitucionalmente imperioso; (ii) está estrechamente vinculada con dicha finalidad y (iii) es la medida menos restrictiva posible? (Test estricto).
221. A continuación, se emprende la contestación a cada una de estas interrogantes.
- a) **Test ordinario sobre la afectación a los derechos a la privacidad y protección de datos personales**
- Fin constitucionalmente válido*
222. El primer aspecto que debe analizarse es si el sistema normativo que permite al Estado a través del PANAUT recopilar, administrar, conservar por tiempo indeterminado y tener acceso a la información privada y los datos personales de toda aquella persona física y/o moral que sea titular de una línea de telefonía móvil, persigue un fin constitucionalmente válido.
223. Sobre este aspecto, conviene citar nuevamente los *Principios del CIJ*, puesto que el *Principio Uno*, referido a las *Finalidades Legítimas y Lealtad*, dispone que “*Los datos personales deberían ser recopilados solamente para finalidades legítimas y por medios legales y legítimos.*”⁹⁰
224. Al respecto, el referido Comité explica que el requisito de legitimidad en las finalidades para las cuales se tratan los datos personales es una norma fundamental, profundamente arraigada en valores democráticos básicos y en el estado de derecho. Abarca el concepto de legalidad y excluye el tratamiento arbitrario y caprichoso de los datos personales, implica transparencia y una estructura jurídica a la cual pueda tener acceso la persona cuyos datos estén recopilándose.
225. Así, el mandato general es que **no deben recopilarse datos sobre las personas excepto en las situaciones y con los métodos permitidos o autorizados por la ley.**
226. Es por eso que se establece que los Estados miembros deben incluir en sus legislaciones nacionales disposiciones específicas sobre las finalidades legítimas del tratamiento de datos personales, los cuales podrían incluir casos en los que: (a) el Titular de los Datos otorgue su consentimiento expreso para el Tratamiento de sus Datos Personales para una o varias finalidades específicas; (b) el Tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales; (c) el Tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al Responsable de datos; (d) el Tratamiento sea necesario para proteger intereses vitales del Titular o de otra persona; (e) el Tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al Responsable de Datos; (f) el Tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el Responsable de Datos; (g) el Tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente; y (h) el Tratamiento sea necesario para el reconocimiento o defensa de los derechos del Titular ante una autoridad pública.

⁸⁹ Cabe precisar que a esta misma conclusión llegó el Tribunal Pleno al resolver la acción de inconstitucionalidad 21/2013, resuelta por sentencia de tres de julio de dos mil catorce. En dicho asunto se analizó la constitucionalidad del artículo 275 Bis del Código de Procedimientos Penales del Estado de Nuevo León al regular la prueba de ADN como método de identificación de los testigos. EL precepto fue declarado inconstitucional por unanimidad de diez votos de los señores Ministros Gutiérrez Ortiz Mena, Cossío Díaz con precisiones en cuanto a las consideraciones, Luna Ramos en contra de las consideraciones, Franco González Salas con precisiones en cuanto a las consideraciones, Zaldivar Lelo de Larrea, Pardo Rebolledo con precisiones en cuanto a las consideraciones, Aguilar Morales con precisiones en cuanto a las consideraciones, Valls Hernández con precisiones en cuanto a las consideraciones, Pérez Dayán y Presidente Silva Meza.

⁹⁰ Adoptados mediante resolución CJI/RES.266 (XCVIII/21), de nueve de abril de dos mil veintiuno.

227. Al respecto, el Comité señala que, en principio, la recopilación de los datos personales debe limitarse a aquellos casos en los que se cuenta con el consentimiento de la persona, salvo delimitadas excepciones.⁹¹ Complementa esta regulación el *Principio Dos* referido a la *Transparencia y Consentimiento*, el cual establece lo siguiente:

“Antes o en el momento en que se recopilen, se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para los cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados. Cuando el procesamiento se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento previo, libre, inequívoco e informado de la persona a que se refieran.”

228. Sobre este punto, expresa el Comité que **por regla general** las personas deben tener la posibilidad de dar su consentimiento de forma libre respecto a la recopilación de sus datos personales, por lo tanto, el consentimiento debe basarse en información suficiente y ser claro, es decir, no dar lugar a ninguna duda o ambigüedad con respecto a su intención. El titular debe ser capaz de efectuar una elección real y no debe correr ningún riesgo de engaño, intimidación, coacción o consecuencia negativa significativa si se niega a dar su consentimiento.
229. Solo **por excepción** es posible autorizar la recopilación de datos personales sin necesidad del consentimiento de su titular, cuando el responsable cuente con fundamentos legales alternativos, establecidos en el derecho interno o en el derecho internacional. En esos casos, la parte que procure recopilar y tratar los datos debe demostrar que tiene una necesidad clara de hacerlo para proteger sus intereses legítimos o los de un tercero a quien puedan divulgarse los datos. También se debe demostrar que hay un equilibrio entre los intereses legítimos de la parte que busque la divulgación y los intereses del titular de los datos.
230. Se relata como ejemplo el contexto de la acción humanitaria, en el cual obtener el consentimiento puede ser muy difícil y, por ende, puede ser necesario y legítimo recurrir a otro fundamento jurídico, como el interés público o los intereses vitales del titular de datos. Este puede ser el caso, por ejemplo, cuando el tratamiento de datos personales es un prerrequisito para recibir asistencia, o cuando se requieran recopilar los datos de una persona desaparecida. En estos casos, las organizaciones humanitarias deberían fundamentar y motivar claramente su recopilación.
231. El parámetro es aún más contundente tratándose de datos sensibles, pues respecto a ellos el Comité señala que solamente deberían procesarse sin el consentimiento explícito de su titular, en los casos en que ello sea claramente de gran interés público (según lo que esté autorizado por ley) o responda a intereses vitales del titular de los datos (por ejemplo, en una situación de emergencia en la cual corra peligro su vida).
232. De lo anterior, es posible advertir que desde el ámbito internacional la **regla general** es que para poder llevar a cabo el tratamiento de datos personales es necesario contar con el **consentimiento** real, libre e informado de su titular, lo cual guarda perfecta congruencia con la denominada *autodeterminación informativa*.
233. En consecuencia, **solo por excepción** el tratamiento de datos personales puede darse sin necesidad de contar con el consentimiento de su titular, siempre que se sustente en causas legítimas como el cumplimiento de una misión realizada en interés público que sea razonable y compatibles con los derechos y libertades, cuando el tratamiento sea necesario para la satisfacción de intereses legítimos, o bien cuando sea en claro beneficio del propio titular. Sin embargo, debe precisarse que, al tratarse de excepciones a la regla general, estos supuestos deben ser interpretados de forma restringida.
234. Al respecto los *Principios del CIJ*, concretamente el *Principio Doce* de las *Excepciones*, establece lo siguiente:

“Cualquier excepción a alguno de estos Principios debería estar prevista de manera expresa y específica en la legislación nacional, ser puesta en conocimiento del público y limitarse únicamente a motivos relacionados con la soberanía nacional, la seguridad nacional, la seguridad pública, la protección de la salud pública, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público o el interés público.”

⁹¹ Sobre estos comentarios, véase “*Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con anotaciones*”, páginas 7 y 8.

235. El Comité Jurídico Interamericano explica sobre este punto que en algunos casos es posible que las autoridades de los Estados tengan que apartarse de estos Principios o establecer restricciones, sin embargo, estos casos deben limitarse a los necesarios, adecuados y proporcionales en una sociedad democrática que permitan salvaguardar la seguridad nacional y la seguridad pública, la protección de la salud pública, la administración de justicia, el cumplimiento de la normativa u otras prerrogativas esenciales del orden público, o la protección de los derechos y libertades de otros objetivos de interés público general. Por ejemplo, al responder a las amenazas planteadas por la delincuencia internacional, el terrorismo y la corrupción, así como a ciertas violaciones graves a los derechos humanos.
236. Sin embargo, estas excepciones y desviaciones respecto a los principios deben ser la excepción y no la regla. Deben aplicarse solo después de considerar lo más cuidadosamente posible la importancia de proteger la privacidad individual, la dignidad y el honor, respetando los derechos y las libertades fundamentales de los titulares. Debiendo haber límites sensatos en la capacidad de las autoridades nacionales para compeler a los responsables a dar a conocer datos personales, manteniendo un equilibrio entre la necesidad de los datos en circunstancias limitadas y el debido respeto al derecho de los intereses de las personas en materia de privacidad.
237. Además, se precisa que cualquier legislación que tenga como propósito restringir la aplicación de estos Principios debe contener como mínimo, disposiciones relativas a la finalidad del tratamiento, las categorías de datos personales de que se trate, el alcance de las limitaciones establecidas, las garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas, la determinación del responsable, los plazos de conservación de los datos personales, los posibles riesgos para los derechos y libertades de los titulares, y el derecho de los titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta. Las autoridades nacionales deberían poner tales leyes o normas en conocimiento del público a la brevedad posible.⁹²
238. Prácticamente estas mismas directrices se encuentran plasmadas en los numerales 6, 7, 11 y 17 de los *Estándares Iberoamericanos*.
239. Cabe precisar que estos parámetros han sido incorporados en nuestro derecho interno. El artículo 16, párrafo segundo, de la Constitución General reconoce supuestos de excepción a los principios que rigen el tratamiento de datos personales, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger derechos de terceros.
240. Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados es coincidente con estos lineamientos internacionales, pues en su artículo 6 se establece que el Estado deberá garantizar la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente. Sin embargo, también se reconoce que el derecho a la protección de los datos personales **podrá limitarse** solamente por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas y para proteger los derechos de terceros.⁹³
241. El artículo 18 establece que todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.⁹⁴

⁹² *Ibidem*, páginas 28 y 29.

⁹³ Artículo 6. El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

⁹⁴ Artículo 18. Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

El responsable podrá tratar datos personales para finalidades distintas a aquellas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

242. En ese sentido, el artículo 20 señala que, por regla general, para poder realizar el tratamiento de datos personales la autoridad responsable deberá contar con el consentimiento previo de su titular,⁹⁵ previéndose en el artículo 22 los casos de excepción a esta regla, destacando la fracción I, referida a los casos en los que la ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la propia legislación.⁹⁶
243. Finalmente, el artículo 80 refiere que la obtención y tratamiento de datos personales por parte de las instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos.⁹⁷
244. Similares mandatos se encuentran previstos en los artículos 8, 9 y 10 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.
245. En esa tesitura, debe recordarse un aspecto que ya se mencionó anteriormente. La recopilación, administración, conservación y acceso a la información privada y los datos personales de los usuarios de telefonía móvil que se otorga al Estado y a particulares través del PANAUT **no está basada en el consentimiento**, dado que no resulta optativo para dichos usuarios proporcionar o no la información requerida, sino más bien se les impone como una **condición obligatoria** a fin de poder *adquirir* o *conservar* el servicio de telefonía móvil. Además, el consentimiento del usuario tampoco interviene en el uso y destino que se le dará a su información, ni tampoco sobre quién podrá acceder a ella, pues estos aspectos ya vienen predeterminados por la norma.
246. En consecuencia, lo que debe analizarse a la luz de los lineamientos y estándares anteriormente expuestos es si la finalidad que persiguió el legislador para recopilar, almacenar y administrar la información privada y los datos personales de los usuarios de telefonía móvil a través del PANAUT, aún sin su consentimiento, es legítima, esto es, si cae en alguno de los casos de excepción que justifican este tipo de tratamiento de datos.
247. Este Tribunal Pleno estima que sí, en atención a las siguientes consideraciones.
248. El párrafo primero del artículo 180 bis impugnado declara expresamente que la única finalidad que persigue el PANAUT es colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos⁹⁸.
249. Del proceso legislativo que dio lugar a la expedición del Decreto impugnado se desprende con claridad que la necesidad de emitir esta regulación se debió al aumento exponencial de ciertos delitos que se cometen a través de la utilización de equipos móviles, destacándose de entre ellos, los delitos de secuestro y extorsión.
250. Se señaló que el combate y erradicación de estas conductas ha sido especialmente complicado ya que los métodos de ejecución son vía remota mediante el uso de teléfonos móviles desechables, lo que impide tanto la identificación del titular de la línea como su geolocalización, de ahí la urgente necesidad de generar mecanismos varios encaminados a reducir drásticamente las actividades de las organizaciones del crimen organizado que operan bajo estas modalidades.

⁹⁵ Artículo 20. Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

I. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;

II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e

III. Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

⁹⁶ Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;

(...)

⁹⁷ Artículo 80. La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de los sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto.

Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en el presente Capítulo.

⁹⁸ Artículo 180 Bis. El Instituto expedirá las disposiciones administrativas de carácter general para la debida operación del Padrón Nacional de Usuarios de Telefonía Móvil, el cual es una base de datos con información de las personas físicas o morales titulares de cada línea telefónica móvil que cuenten con número del Plan Técnico Fundamental de Numeración **y cuyo único fin 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.

251. En consecuencia, se creyó conveniente la creación de este Padrón Nacional de Usuarios de Telefonía Móvil bajo la operación y vigilancia del Instituto Federal de Telecomunicaciones, como una herramienta útil en la búsqueda permanente de inhibir la comisión de este tipo de delitos, así como una valiosa plataforma para lograr un mayor éxito en las investigaciones de las autoridades encargadas de la seguridad y de la administración y procuración de justicia en nuestro país, lo que se estimó redundaría en una mayor certeza y seguridad jurídica para la ciudadanía en su conjunto.
252. El legislador optó por diseñar un esquema de registro para así tener conocimiento de quiénes son los titulares de las líneas telefónicas, otorgando a las autoridades competentes mayores elementos normativos para identificar a los responsables cuando se cometan ilícitos a través del uso de estos equipos móviles. Así, se pretende que cuando algún delincuente utilice un número para secuestro, extorsión o algún otro delito, la autoridad pueda acceder mediante la base de datos de las compañías de telecomunicaciones a los datos registrados de dichas líneas y así poder identificar con mayor facilidad a sus autores.
253. De estas consideraciones, se puede advertir que la medida legislativa impugnada persigue *finés de orden público* relacionados con el fortalecimiento de las herramientas para la investigación y persecución de los delitos. Concretamente, con la creación del PANAUT se buscó generar una base de datos asociada a la titularidad de las líneas de telefonía móvil, que permitiera investigar y perseguir de mejor manera las conductas delictivas a través de la identificación de los titulares de las líneas utilizadas para su comisión, por ejemplo, en casos de extorsión o secuestro.
254. En esa tesitura, debe reconocerse que esta finalidad se encuentra inserta en el marco de las obligaciones que el artículo 21 constitucional impone al Estado Mexicano, pues establece que la seguridad pública es una función a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social.
255. Sobre el particular, esta Suprema Corte de Justicia ha establecido que la función estatal de seguridad pública tiene por objeto garantizar condiciones adecuadas para que las personas ejerzan sus derechos, por lo que deben establecerse mecanismos mediante los cuales se logre prevenir, remediar o eliminar aquellas situaciones de violencia en contra de las personas, su vida, libertad, propiedad y demás derechos.⁹⁹
256. Inclusive, se ha reconocido que la investigación y persecución de los delitos también guarda relación con el acceso a la impartición de justicia, ya que, si bien en términos del artículo 17 constitucional, ésta se refiere a la función jurisdiccional desarrollada por los tribunales, lo cierto es que tiene como

⁹⁹ Registro digital: 192083, Instancia: Pleno, Novena Época, Materias(s): Constitucional, Tesis: P./J. 35/2000, Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XI, Abril de 2000, página 557, Tipo: Jurisprudencia
SEGURIDAD PÚBLICA. SU REALIZACIÓN PRESUPONE EL RESPETO AL DERECHO Y EN ESPECIAL DE LAS GARANTÍAS INDIVIDUALES. Del análisis sistemático de los artículos 16, 21, 29, 89, fracción VI, 129 y 133, de la Constitución, así como 2o., 3o., 5o., 9o., 10, 13 y 15, de la Ley General que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública; 1o., 2o., 3o., 10 y 11, de la Ley Orgánica del Ejército y Fuerza Aérea Mexicanos, y 1o., 2o., 9o. y 10, de la Ley Orgánica de la Armada de México, se deduce que el Estado mexicano, a través de sus tres niveles de gobierno y de todas las autoridades que tengan atribuciones relacionadas, directa o indirectamente, con la seguridad pública, deben coadyuvar a lograr los objetivos de ésta, traducidos en libertad, orden y paz pública, como condiciones imprescindibles para gozar de las garantías que la Constitución reconoce a los gobernados. El examen de los diferentes preceptos citados, con los demás elementos que permiten fijar su alcance, lleva a concluir que, jurídicamente, los conceptos de garantías individuales y seguridad pública no sólo no se oponen sino se condicionan recíprocamente. No tendría razón de ser la seguridad pública si no se buscara con ella crear condiciones adecuadas para que los gobernados gocen de sus garantías; de ahí que el Constituyente Originario y el Poder Reformador de la Constitución, hayan dado las bases para que equilibradamente y siempre en el estricto marco del derecho se puedan prevenir, remediar y eliminar o, al menos disminuir, significativamente, situaciones de violencia que como hechos notorios se ejercen en contra de las personas en su vida, libertad, posesiones, propiedades y derechos. Por ello, sería inadmisibles en el contexto jurídico constitucional interpretar la seguridad pública como posibilidad de afectar a los individuos en sus garantías, lo que daría lugar a acudir a los medios de defensa que la propia Constitución prevé para corregir esas desviaciones. Consecuentemente, por el bien de la comunidad a la que se debe otorgar la seguridad pública, debe concluirse que resulta inadmisibles constitucionalmente un criterio que propicie la proliferación y fortalecimiento de fenómenos que atenten gravemente contra los integrantes del cuerpo social, así como de cualquier otro que favoreciera la arbitrariedad de los órganos del Estado que, so pretexto de la seguridad pública, pudieran vulnerar las garantías individuales consagradas en el Código Supremo. Por tanto, debe establecerse el equilibrio entre ambos objetivos: defensa plena de las garantías individuales y seguridad pública al servicio de aquéllas. Ello implica el rechazo a interpretaciones ajenas al estudio integral del texto constitucional que se traduzca en mayor inseguridad para los gobernados o en multiplicación de las arbitrariedades de los gobernantes, en detrimento de la esfera de derecho de los gobernados.

presupuesto la efectiva investigación de los delitos, de manera que el Estado está obligado a realizar una averiguación seria, imparcial y efectiva, para lo cual debe usar todos los medios legales disponibles.¹⁰⁰

257. En efecto, se ha sostenido en reiteradas ocasiones que la obligación del Estado de investigar debe de cumplirse diligentemente para evitar la impunidad y propiciar que este tipo de hechos no se repitan, por lo que una vez que las autoridades estatales conocen de una probable conducta delictiva, están obligadas a iniciar *ex officio* y sin dilación una investigación seria, imparcial y efectiva por todos los medios legales disponibles y orientada a la determinación de la verdad y a la persecución, captura, enjuiciamiento y eventual castigo de sus autores, ya sean particulares o agentes estatales.¹⁰¹
258. En consecuencia, este Tribunal Pleno considera que dicha finalidad resulta *legítima* para efectos de la recopilación y tratamiento de datos personales, en términos de los estándares expuestos, pues la Constitución General, los instrumentos internacionales citados, como las leyes nacionales en la materia, son coincidentes en establecer que la seguridad pública es un principio de orden público cuya relevancia puede justificar en ciertos casos y bajo el cumplimiento de otras condiciones adicionales, la limitación de los derechos a la privacidad y protección de datos personales.
259. El propio *Principio Uno* de los Principios del CJI, es claro en establecer que cualquier excepción además de estar prevista de manera expresa y específica en la legislación nacional, debe limitarse únicamente a motivos relacionados con la soberanía nacional, la seguridad nacional, **la seguridad pública**, la protección de la salud pública, **el combate a la criminalidad**, el cumplimiento de normativas u otras prerrogativas de orden público o el interés público.
260. En consecuencia, si la finalidad que reconoció el legislador ordinario como justificación para la creación del PANAUT es colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos, a través de la creación de una base de datos asociada a la titularidad de las líneas de telefonía móvil, que permitiera investigar y perseguir de mejor manera las conductas delictivas a través de la identificación de los titulares de las líneas utilizadas para su comisión, debe concluirse que dicha finalidad es *legítima*, pues no solo tiene un fundamento constitucional sino que además, es acorde con los estándares internacionales incorporados en nuestro sistema jurídico.
261. No se deja de advertir que el INAI alega que la finalidad de la medida no es válida en tanto que no busca contribuir en el combate de determinados ilícitos realizados a través del uso de dispositivos móviles, sino que su objeto es la creación de un padrón de datos de todos los mexicanos a fin de poder controlar y supervisar a la población, lo cual no solamente no tiene un sustento constitucional, sino que va directamente en contra de las bases que sostienen un Estado democrático.
262. Contrario a lo que alega el accionante, ni de los trabajos legislativos que dieron lugar a la emisión del Decreto impugnado ni de la regulación contenida en dicho Decreto pueden advertirse elementos suficientes que permitan sostener de manera categórica que la creación de este padrón tiene como intención la de crear un sistema de vigilancia permanente sobre la población.

¹⁰⁰ Registro digital: 163168, Instancia: Pleno, Novena Época, Materias(s): Constitucional, Penal, Tesis: P. LXIII/2010, Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXXIII, Enero de 2011, página 25, Tipo: Aislada DERECHO DE ACCESO A LA JUSTICIA. LA INVESTIGACIÓN Y PERSECUCIÓN DE LOS DELITOS CONSTITUYEN UNA OBLIGACIÓN PROPIA DEL ESTADO QUE DEBE REALIZARSE DE FORMA SERIA, EFICAZ Y EFECTIVA. El derecho de acceso a la justicia previsto en la Constitución Política de los Estados Unidos Mexicanos está referido a la función jurisdiccional desarrollada por los tribunales, pero también debe entenderse vinculado, particularmente en el caso de la justicia penal, con la investigación y persecución de los delitos, función asignada al Ministerio Público conforme a los artículos 21 y 102, apartado A, constitucionales, pues tal prerrogativa tiene como presupuesto lógico, en una relación de interdependencia, la efectiva investigación de los delitos. Esta obligación de investigar y perseguir los actos delictuosos debe asumirse por el Estado como una obligación propia y no como un mero trámite, ni su avance debe quedar a la gestión de los particulares afectados o de sus familiares, sino que realmente debe tratarse de una investigación seria, imparcial y efectiva, utilizando todos los medios legales disponibles que permitan la persecución, captura, enjuiciamiento y, en su caso, sanción a los responsables de los hechos, especialmente cuando están involucrados agentes estatales. Ello es así, porque en el respeto a los derechos fundamentales, particularmente los relativos a la vida y a la integridad física, el Estado debe asumir una conducta activa y decidida para prevenir su vulneración, a través de las acciones legislativas, administrativas y judiciales necesarias, además de acometer lo necesario para que, en caso de ser vulnerados, las conductas respectivas puedan ser sancionadas.

¹⁰¹ Caso de la Masacre de Pueblo Bello Vs. Colombia, Fondo, Reparaciones y Costas. Sentencia de treinta y uno de enero de dos mil seis. Serie C No. 140, párr. 143; Caso Heliodoro Portugal Vs. Panamá, Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de doce de agosto de dos mil ocho. Serie C No. 186, párr. 144, y Caso Valle Jaramillo y otros Vs. Colombia, Fondo, Reparaciones y Costas. Sentencia de veintisiete de noviembre de dos mil ocho. Serie C No. 192, párr. 101; Caso González y Otras ("Campo algodonero") vs. México. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de dieciséis de noviembre de dos mil nueve. Serie C No. 205, párr. 290.

263. Por el contrario, lo que se puede apreciar por parte del legislador ordinario es el reconocimiento de un fenómeno social delictivo que afecta la tranquilidad y seguridad de la sociedad mexicana en su conjunto, por lo que se pensó en generar un mecanismo que fuera útil para combatir dicho fenómeno, específicamente, la generación de una base de datos ligada a la titularidad de las líneas de telefonía móvil, al ser éstas uno de los instrumentos fundamentales para la comisión de ciertos delitos, dada las condiciones de anonimato que proporciona en ciertas modalidades.
264. En esa tesitura, lo que corresponde analizar en este punto de la prueba es únicamente si dicha finalidad es acorde con los principios constitucionales y estándares internacionales, a fin de poder calificarla como válida o legítima. Lo que se reitera, debe contestarse en sentido afirmativo.
265. Sin embargo, sobre esta conclusión conviene aclarar dos cuestiones, que, aunque ya se explicaron, su reiteración se estima importante.
266. La primera es que afirmar que la creación y regulación del PANAUT persigue una finalidad válida y/o legítima, no conduce a sostener en automático que dicho sistema normativo es válido, pues para ello es necesario analizar el resto de las gradas que integran la prueba de proporcionalidad.
267. Esto inclusive es reconocido por los estándares internacionales, pues si bien se reconoce que la seguridad pública es un principio de orden público cuya relevancia permite justificar la limitación de los derechos a la privacidad y protección de datos personales, lo cierto es que la validez de dicha limitación está sujeta también al cumplimiento de condiciones adicionales, que son precisamente las que habrán de verificarse en las siguientes gradas de la prueba.
268. En efecto, si bien la lucha contra la delincuencia reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación, este objetivo de interés general, por fundamental que sea, no puede justificar que una medida de conservación de datos personales se considere necesaria a los efectos de dicha lucha.
269. Y segundo, esta primera conclusión no pretende negar o desconocer que, a pesar de estar justificada en un fin válido o legítimo, la creación de este tipo de base de datos, mal reguladas o implementadas, pueden dar lugar a la generación de sistemas de control y vigilancia permanente de la población, lo cual evidentemente resulta contrario a las bases que sostienen un Estado democrático.
270. Sin embargo, tal aspecto, aunque de gran relevancia, no corresponde analizarlo en este punto del test, pues se reitera, lo único que se examina en esta grada es si la finalidad o las razones que justifican la medida legislativa pueden calificarse como válidas o legítimas. Será en las siguientes gradas en las que se analice si las condiciones en las que se regula el PANAUT resultan adecuadas para evitar que la afectación a los derechos a la privacidad y protección de datos personales de los usuarios de telefonía móvil sea innecesaria o desproporcionales y, por tanto, se torne en una figura de abuso que vaya en contra de los derechos de las personas.

Idoneidad de la medida

271. En esta segunda grada corresponde analizar si la medida legislativa que crea el PANAUT y que permite recopilar, administrar, conservar por tiempo indeterminado y tener acceso a la información privada y los datos personales de toda aquella persona física y/o moral que sea titular de una línea de telefonía móvil, es una medida *idónea* para fortalecer la seguridad pública a través del combate de los delitos.
272. Como se explicó anteriormente, el examen de idoneidad presupone la existencia de una relación instrumental entre la intervención al derecho y el fin que persigue dicha afectación, siendo suficiente que la medida contribuya *en algún modo y en algún grado* a lograr el propósito que busca el legislador. En otras palabras, bajo un escrutinio ordinario, no es necesario que la medida adoptada sea la óptima en términos de relación medio a fin, sino que basta con que contribuya de algún modo a la consecución de la finalidad identificada.
273. En esa tesitura, debe decirse que el sistema normativo impugnado **supera esta segunda grada de la prueba de proporcionalidad**, pues se reconoce que existe una relación de medio-fin entre la creación del PANAUT y el combate de aquellos delitos cometidos a través de la utilización de dispositivos móviles.
274. Esto, porque contar con una base de datos que identifica a los titulares de las líneas de telefonía móvil, aunque genera una afectación a la privacidad y la protección de los datos personales de los usuarios, lo cierto es que en principio, es susceptible de otorgar un mayor control sobre el uso de estos dispositivos ya que puede facilitar la identificación de las personas titulares de las líneas, lo que contrarresta en cierta medida esta barrera del anonimato que es la que da pie a que estos mecanismos sean vistos como herramientas útiles y seguras para la comisión de ciertos delitos.

275. En esa medida, debe reconocerse la relación instrumental que existe entre la creación del PANAUT y el fortalecimiento de la seguridad pública a través del combate a la delincuencia, pues resulta razonable afirmar que esta base de datos *puede servir para identificar con mayor facilidad a quienes utilicen estos dispositivos para cometer delitos, contribuyendo de algún modo a inhibir esta clase de conductas*. En consecuencia, la medida legislativa satisface esta segunda grada de la prueba de proporcionalidad.
276. No se deja de advertir que el INAI sostiene que esta medida no es idónea para el fin perseguido, pues señala que los propios legisladores reconocieron que no existe evidencia contundente que demuestre que esta clase de registros impacte en la reducción de los delitos de extorsión y secuestro, por el contrario, experiencias anteriores han demostrado que este tipo de mecanismos no contribuye en nada en el combate de estas conductas sino que dan lugar a abusos y afectaciones a los derechos humanos de los usuarios.
277. Al respecto debe decirse que no asiste la razón a dicho Instituto, pues como ha quedado señalado, el análisis de idoneidad desde un escrutinio ordinario no implica analizar si la medida adoptada por el legislador es la mejor de las medidas posibles, o si es plenamente eficaz para la consecución de la finalidad que persigue.
278. Por el contrario, lo único que corresponde examinar en esta grada es si existe una relación de instrumentalidad entre la medida legislativa analizada y el fin constitucionalmente válido que se persigue, esto es, si la medida contribuye *en alguna medida* a la satisfacción de dicha finalidad, condición que como vimos, sí se satisface en el caso concreto, pues resulta razonable inferir que tener una base con los datos que identifiquen a cada titular de una línea de telefonía móvil se conecta con la investigación de los delitos que se comenten a través de la utilización de estos dispositivos, lo que puede repercutir en la disminución de este tipo de conductas al impactar en el anonimato que el uso de estos mecanismos suele otorgar.
279. En consecuencia, se concluye que la medida legislativa impugnada es idónea para la consecución de la finalidad legítima previamente identificada.
- Necesidad de la medida
280. Corresponde ahora analizar si la creación del PANAUT que permite recopilar, administrar, conservar por tiempo indeterminado y tener acceso a la información privada y los datos personales de toda aquella persona física y/o moral que sea titular de una línea de telefonía móvil es una medida *necesaria* para la seguridad pública y en concreto, para combatir de mejor manera los delitos que se cometen a través del uso de estos dispositivos.
281. Debe recordarse que este concepto de necesidad también se encuentra reconocido en el plano internacional, pues la Corte Interamericana de Derechos Humanos ha establecido que el derecho a la privacidad, como cualquier otro derecho, no es absoluto, por lo que puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias. Por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, **necesidad** y proporcionalidad, es decir, deben ser **necesarias** en una sociedad democrática.¹⁰²
282. Ahora bien, tal y como se expuso anteriormente, el examen de necesidad implica corroborar en primer lugar, si existen otras medidas o mecanismos que resulten igualmente idóneos para lograr los fines que se persiguen y, en segundo lugar, determinar si estas alternativas intervienen con menor intensidad el derecho fundamental afectado. Así, de encontrarse alguna medida alternativa que sea igualmente idónea para proteger el fin constitucional y que a su vez intervenga con menor intensidad al derecho, deberá concluirse que la medida elegida por el legislador es inconstitucional.
283. En consecuencia, la pregunta que debe responderse en el presente apartado es la siguiente: *¿existen otro tipo de medidas distintas del PANAUT que resulten igualmente idóneas para el fortalecimiento de la seguridad pública a través del combate de los delitos que se cometen mediante el uso de dispositivos de telefonía móvil, pero que resultan menos restrictivas de los derechos a la privacidad y protección de los datos personales?*
284. Este Tribunal Pleno considera que **sí existen** y, para justificar esta conclusión, resulta conveniente transcribir los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, y 252, 291, 292, 293, 294, 298, 299, 300, 301, 302 y 303 del Código Nacional de Procedimientos Penales, los cuales establecen lo siguiente:

¹⁰² Cfr. Caso *Tristán Donoso Vs. Panamá*, Sentencia de veintisiete de enero de dos mil nueve, párr. 56 y Caso *Escher y otros Vs. Brasil*, Sentencia de seis de julio dos mil nueve, párr. 116

Ley Federal de Telecomunicaciones y Radiodifusión

Artículo 189. Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes.

Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.

Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

I. Colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes.

Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable.

El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta Ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna;

II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

- a) Nombre, denominación o razón social y domicilio del suscriptor;
- b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);
- c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;
- d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;
- e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;
- f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;
- g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y
- h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se refiere el artículo 189 de esta Ley, los cuales deberán informarse al Instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.

Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

III. Entregar los datos conservados a las autoridades a que se refiere el artículo 189 de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables.

Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a entregar la información dentro de un plazo máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente;

IV. Contar con un área responsable disponible las veinticuatro horas del día y los trescientos sesenta y cinco días del año, para atender los requerimientos de información, localización geográfica e intervención de comunicaciones privadas a que se refiere este Título.

Para efectos de lo anterior, los concesionarios deberán notificar a los titulares de las instancias a que se refiere el artículo 189 de esta Ley el nombre del responsable de dichas áreas y sus datos de localización; además deberá tener facultades amplias y suficientes para atender los requerimientos que se formulen al concesionario o al autorizado y adoptar las medidas necesarias. Cualquier cambio del responsable deberá notificarse previamente con una anticipación de veinticuatro horas;

V. Establecer procedimientos expeditos para recibir los reportes de los usuarios del robo o extravío de los equipos o dispositivos terminales móviles y para que el usuario acredite la titularidad de los servicios contratados. Dicho reporte deberá incluir, en su caso, el código de identidad de fabricación del equipo;

VI. Realizar la suspensión del servicio de los equipos o dispositivos terminales móviles reportados como robados o extraviados, a solicitud del titular, y realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil.

Los concesionarios deberán celebrar convenios de colaboración que les permitan intercambiar listas de equipos de comunicación móvil reportados por sus respectivos clientes o usuarios como robados o extraviados, ya sea que los reportes se hagan ante la autoridad competente o ante los propios concesionarios;

VII. Realizar el bloqueo inmediato de líneas de comunicación móvil que funcionen bajo cualquier esquema de contratación reportadas por los titulares o propietarios, utilizando cualquier medio, como robadas o extraviadas, y proceder a realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil; así como, realizar la suspensión inmediata del servicio de telefonía móvil cuando así lo instruya el Instituto para efectos del Padrón Nacional de Usuarios de Telefonía Móvil o la autoridad competente para hacer cesar la comisión de delitos, de conformidad con lo establecido en las disposiciones administrativas y legales aplicables;

VIII. Colaborar con las autoridades competentes para que en el ámbito técnico operativo se cancelen o anulen de manera permanente las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen dentro del perímetro de centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores, federales o de las entidades federativas, cualquiera que sea su denominación.

El bloqueo de señales a que se refiere el párrafo anterior se hará sobre todas las bandas de frecuencia que se utilicen para la recepción en los equipos terminales de comunicación y en ningún caso excederá de veinte metros fuera de las instalaciones de los centros o establecimientos a fin de garantizar la continuidad y seguridad de los servicios a los usuarios externos. En la colaboración que realicen los concesionarios se deberán considerar los elementos técnicos de reemplazo, mantenimiento y servicio.

Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a colaborar con el Sistema Nacional de Seguridad Pública en el monitoreo de la funcionalidad u operatividad de los equipos utilizados para el bloqueo permanente de las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen;

IX. Implementar un número único armonizado a nivel nacional y, en su caso, mundial para servicios de emergencia, en los términos y condiciones que determine el Instituto en coordinación con el Sistema Nacional de Seguridad Pública, bajo plataformas interoperables, debiendo contemplar mecanismos que permitan identificar y ubicar geográficamente la llamada y, en su caso, mensajes de texto de emergencia;

X. Informar oportuna y gratuitamente a los usuarios el o los números telefónicos asociados a los servicios de seguridad y emergencia que determine el Instituto en coordinación con el Sistema Nacional de Seguridad Pública, así como proporcionar la comunicación a dichos servicios de forma gratuita;

XI. En los términos que defina el Instituto en coordinación con las instituciones y autoridades competentes, dar prioridad a las comunicaciones con relación a situaciones de emergencia, y

XII. Realizar bajo la coordinación del Instituto los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualización de riesgos o amenazas a la seguridad nacional. Los concesionarios que operen redes públicas de telecomunicaciones podrán voluntariamente constituir una organización que tenga como fin la realización de los citados estudios e investigaciones. Los resultados que se obtengan se registrarán en un informe anual que se remitirá al Instituto, al Congreso de la Unión y al Ejecutivo Federal.

Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.

Código Nacional de Procedimientos Penales

Artículo 252. *Actos de investigación que requieren autorización previa del Juez de control*

Con excepción de los actos de investigación previstos en el artículo anterior, requieren de autorización previa del Juez de control todos los actos de investigación que impliquen afectación a derechos establecidos en la Constitución, así como los siguientes:

I. La exhumación de cadáveres;

II. Las órdenes de cateo;

III. La intervención de comunicaciones privadas y correspondencia;

IV. La toma de muestras de fluido corporal, vello o cabello, extracciones de sangre u otros análogos, cuando la persona requerida, excepto la víctima u ofendido, se niegue a proporcionar la misma;

V. El reconocimiento o examen físico de una persona cuando aquélla se niegue a ser examinada, y

VI. Las demás que señalen las leyes aplicables.

Artículo 291. Intervención de las comunicaciones privadas

Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Procuraduría General de la República, o en quienes éste delegue esta facultad, así como los Procuradores de las entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.

La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.

La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido.

También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos.

Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público.

Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial.

Artículo 292. Requisitos de la solicitud

La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención.

El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.

Artículo 293. Contenido de la resolución judicial que autoriza la intervención de las comunicaciones privadas

En la autorización, el Juez de control determinará las características de la intervención, sus modalidades, límites y en su caso, ordenará a instituciones públicas o privadas modos específicos de colaboración.

Artículo 294. Objeto de la intervención

Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

En ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su Defensor.

El Juez podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.

Artículo 298. Registro

El registro a que se refiere el artículo anterior contendrá las fechas de inicio y término de la intervención, un inventario pormenorizado de los documentos, objetos y los medios para la reproducción de sonidos o imágenes captadas durante la misma, cuando no se ponga en riesgo a la investigación o a la persona, la identificación de quienes hayan participado en los actos de investigación, así como los demás datos que se consideren relevantes para la investigación. El registro original y el duplicado, así como los documentos que los integran, se numerarán progresivamente y contendrán los datos necesarios para su identificación.

Artículo 299. Conclusión de la intervención

Al concluir la intervención, la Policía o el perito, de manera inmediata, informará al Ministerio Público sobre su desarrollo, así como de sus resultados y levantará el acta respectiva. A su vez, con la misma prontitud el Ministerio Público que haya solicitado la intervención o su prórroga lo informará al Juez de control.

Las intervenciones realizadas sin las autorizaciones antes citadas o fuera de los términos en ellas ordenados, carecerán de valor probatorio, sin perjuicio de la responsabilidad administrativa o penal a que haya lugar.

Artículo 300. Destrucción de los registros

El Órgano jurisdiccional ordenará la destrucción de aquellos registros de intervención de comunicaciones privadas que no se relacionen con los delitos investigados o con otros delitos que hayan ameritado la apertura de una investigación diversa, salvo que la defensa solicite que sean preservados por considerarlos útiles para su labor.

Asimismo, ordenará la destrucción de los registros de intervenciones no autorizadas o cuando éstos rebasen los términos de la autorización judicial respectiva.

Los registros serán destruidos cuando se decrete el archivo definitivo, el sobreseimiento o la absolución del imputado. Cuando el Ministerio Público decida archivar temporalmente la investigación, los registros podrán ser conservados hasta que el delito prescriba.

Artículo 301. Colaboración con la autoridad

Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con las disposiciones aplicables. Asimismo, 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.

El incumplimiento a este mandato será sancionado conforme a las disposiciones penales aplicables.

Artículo 302. Deber de secrecía

Quienes participen en alguna intervención de comunicaciones privadas deberán observar el deber de secrecía sobre el contenido de las mismas.

Artículo 303. Localización geográfica en tiempo real y solicitud de entrega de datos conservados

Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente.

En la solicitud se expresarán los equipos de comunicación móvil relacionados con los hechos que se investigan, señalando los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, su duración y, en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas, números o aparatos que serán objeto de la medida.

La petición deberá ser resuelta por la autoridad judicial de manera inmediata por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público.

Si la resolución se emite o registra por medios diversos al escrito, los puntos resolutivos de la orden deberán transcribirse y entregarse al Ministerio Público.

En caso de que el Juez de control niegue la orden de localización geográfica en tiempo real o la entrega de los datos conservados, el Ministerio Público podrá subsanar las deficiencias y solicitar nuevamente la orden o podrá apelar la decisión. En este caso la apelación debe ser resuelta en un plazo no mayor de doce horas a partir de que se interponga.

Excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria. A partir de que se haya cumplimentado el requerimiento, el Ministerio Público deberá informar al Juez de control competente por cualquier medio que garantice su autenticidad, dentro del plazo de cuarenta y ocho horas, a efecto de que ratifique parcial o totalmente de manera inmediata la subsistencia de la medida, sin perjuicio de que el Ministerio Público continúe con su actuación.

Cuando el Juez de control no ratifique la medida a que hace referencia el párrafo anterior, la información obtenida no podrá ser incorporada al procedimiento penal.

Asimismo el Procurador, o el servidor público en quien se delegue la facultad podrá requerir a los sujetos obligados que establece la Ley Federal de Telecomunicaciones y Radiodifusión, la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata. La solicitud y entrega de los datos contenidos en redes, sistemas o equipos de informática se llevará a cabo de conformidad por lo previsto por este artículo. Lo anterior sin menoscabo de las obligaciones previstas en materia de conservación de información para las concesionarias y autorizados de telecomunicaciones en términos del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión.

285. Del análisis de estos preceptos se puede advertir la existencia de diversas figuras diseñadas como herramientas tecnológicas de investigación que, precisamente por su función, buscan contribuir con las autoridades de seguridad y procuración de justicia a fin de fortalecer la seguridad pública a través de la persecución y el combate a la delincuencia.
286. En esa tesitura, siguiendo la metodología que impone esta grada de la prueba de proporcionalidad, en los siguientes párrafos se realizará un análisis comparativo de estas medidas en relación con el PANAUT, esto con el fin de verificar si son igualmente idóneas para satisfacer la finalidad que ha sido identificada en los apartados anteriores, pero menos restrictivas de los derechos a la privacidad y protección de datos personales de los usuarios de telefonía móvil.
287. Sobre este particular, resulta de la mayor importancia puntualizar que el estudio que se desarrolla en los siguientes apartados **no tiene por objeto revisar la validez constitucional de las diversas figuras, ni compromete en sentido alguno el criterio de este Tribunal Pleno sobre tal aspecto**, puesto que lo único que se pretende realizar es un estudio comparativo frente al PANAUT a fin de poder determinar si dichos mecanismos resultan igualmente idóneos, pero son menos restrictivos de los derechos humanos a la privacidad y protección de datos personales. De ahí que se reitera, este Tribunal Pleno no compromete su criterio sobre la validez de las distintas figuras que se mencionan en este apartado y que, desde luego, no son objeto de impugnación en estas acciones de inconstitucionalidad.

288. **Intervención de comunicaciones.** Esta figura constituye una excepción al principio de inviolabilidad de las comunicaciones privadas previsto en el artículo 16 de la Constitución General.¹⁰³
289. De los artículos 252, 291 a 294 y 298 a 302 del Código Nacional de Procedimientos Penales se desprende que esta técnica de investigación busca obtener, a partir de la autorización de un juez, la información generada en los procesos de comunicación entre particulares sea oral, escrita, por signos, señales, mediante el uso de aparatos eléctricos, electrónicos, mecánicos, alámbricos o por cualquier medio que permita dicha comunicación, sea existente o fruto de la evolución tecnológica.
290. Así, se permite que las autoridades de seguridad y procuración de justicia tengan acceso al intercambio de datos e información generada en estos procesos comunicativos, tales como audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación.
291. Además, esta figura permite que pueda llevarse a cabo *la extracción de información*, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos.
292. A la luz de estas generalidades, la primera pregunta que surge es: *¿puede considerarse que esta medida resulta igualmente idónea para colaborar con las autoridades de justicia, en relación con la comisión de delitos mediante el uso de dispositivos de telefonía móvil?*
293. Para este Tribunal la respuesta es afirmativa, pues como se indicó, esta figura otorga a las autoridades el acceso a toda aquella información que se hubiera generado en una comunicación entre particulares, en ese sentido, si el uso de un determinado dispositivo móvil se encuentra relacionado con la comisión de algún ilícito penal, esta medida permite que las autoridades de seguridad y procuración de justicia puedan acceder no solo al nombre y domicilio del suscriptor¹⁰⁴ y a las comunicaciones entabladas por medio de dicho dispositivo, sino que además les permite *extraer* toda la información que en él se contenga, lo que permite aportar una serie de datos que puede ser de gran utilidad tanto para la investigación de la conducta, la identificación de los autores, como para el fincamiento de las responsabilidades.
294. En ese sentido, debe reconocerse la relación de instrumentalidad que existe entre esta herramienta y la investigación y persecución de los delitos, incluyendo aquellos que se cometen mediante el uso de un celular. Sin embargo, la pregunta que naturalmente surge es: *¿resulta igualmente idónea esta medida para la investigación de este tipo de delitos de lo que resulta el PANAUT?*
295. Para este Tribunal Pleno sí lo es, puesto que derivado de sus características, resulta razonable afirmar que intervenir las comunicaciones privadas de quienes pudieran estar relacionados con la comisión de algún delito en el que se usó un dispositivo móvil, así como la extracción de toda la información contenida en ese dispositivo, permite obtener una serie de información o datos que por su naturaleza, resultan de gran utilidad y valor a fin de poder identificar a los sujetos activos del delito.
296. Ahora bien, podría pensarse que tener un padrón aun con más datos personales e íntimos de los titulares de las líneas de telefonía móvil constituye una herramienta *más idónea* para poder identificar con mayor facilidad a quienes utilicen este tipo de dispositivos para la comisión de algún delito. De ahí que no pueda estimarse que resulten medidas equivalentes en cuanto a su idoneidad.

¹⁰³ Art. 16.-

(...)

Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Los Poderes Judiciales contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran control judicial, garantizando los derechos de los indicados y de las víctimas u ofendidos. Deberá existir un registro fehaciente de todas las comunicaciones entre jueces y Ministerio Público y demás autoridades competentes.

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio.

(...)

¹⁰⁴ En efecto, como se verá en el apartado siguiente, la Ley ya obliga a los concesionarios y autorizados a conservar ciertos datos de las comunicaciones, con ciertos requisitos de temporalidad, entre los que se encuentran el nombre y domicilio del titular de la línea bajo cualquier modalidad de contratación, en términos del artículo 190, fracción, inciso a), de la ley impugnada.

297. Sin embargo, este Tribunal Pleno no comparte dicha perspectiva. Primero, porque un razonamiento así estaría basado en una suposición, pues en realidad *nada garantiza* que con este padrón efectivamente se vaya a identificar a los responsables de los delitos, básicamente porque resulta muy complicado sostener que estamos ante una herramienta infalible. Por el contrario, los antecedentes de esta figura permiten advertir que la delincuencia difícilmente va a emplear dispositivos que se encuentran registrados.
298. En efecto, este Tribunal Pleno advierte que no es la primera vez que el legislador ordinario plantea el establecimiento de este tipo de mecanismos. El dos de febrero de dos mil nueve se publicó en el Diario Oficial de la Federación la reforma a diversas disposiciones de la abrogada Ley Federal de Telecomunicaciones, entre ellos el artículo 44, fracción XI, el cual establecía lo siguiente:

Artículo 44. Los concesionarios de redes públicas de telecomunicaciones deberán:

I. a X...

XI. Llevar un registro y control separado de sus usuarios, tanto en la modalidad de líneas contratadas en plan tarifario, como en líneas de prepago, el cual contenga como mínimo los siguientes datos:

a) Número y modalidad de la línea telefónica;

b) Nombre completo, domicilio, nacionalidad, número correspondiente y demás datos contenidos en identificación oficial vigente con fotografía, así como comprobante de domicilio actualizado del usuario y toma de impresión de huella dactilar directamente en tinta y/o electrónicamente;

c) En caso de personas morales, además de los datos de los incisos a) y b), se deberá registrar la razón social de la empresa, cédula fiscal y copia del documento que acredite capacidad para contratar.

Los concesionarios deberán conservar copias fotostáticas o en medios electrónicos de los documentos necesarios para dicho registro y control; así como mantener la reserva y protección de las bases de datos personales, las cuales no podrán ser usadas con fines diferentes a los señalados en las leyes;

299. Del proceso legislativo que dio origen a dicha reforma, se desprende que las razones que las sustentaron fueron muy similares a las que ahora se formularon para justificar la creación del PANAUT. En efecto, se expuso que la implementación de este mecanismo –denominado Registro Nacional de Usuarios de Telefonía Móvil (RENAUT)– constituía la respuesta ante el crecimiento de los delitos cometidos a través del uso de dispositivos de telefonía móvil, de tal suerte que lo que se buscó fue la creación de una base de datos que permitiera la identificación y ubicación de los usuarios que utilizaran la red telefónica como medio para cometer estos ilícitos.
300. Sin embargo, el diecisiete de abril de dos mil doce, la fracción XI del artículo 44 de la anterior Ley Federal de Telecomunicaciones **fue derogada**. De las exposiciones de motivos que dieron lugar a la eliminación de este mecanismo se pueden encontrar las siguientes motivaciones:

“Lo cierto es que la creación del Registro Nacional de Usuarios de Telefonía Móvil (RENAUT) no ha rendido frutos en la prevención, investigación y persecución de delitos como el secuestro y la extorsión. Diversos estudios demuestran que dichos fenómenos delictivos continúan en aumento y que el uso de teléfonos móviles para cometerlos sigue siendo común. De acuerdo con datos del Sistema Nacional de Seguridad Pública, por ejemplo, en 2010 el número de secuestros se incrementó en más de 8% con respecto a 2009. Y según cifras de la organización México Unido Contra la Delincuencia, por cada plagio denunciado ocurren ocho más.

Un dato adicional: antes de la implementación del RENAUT, se registraban cerca de 4,400 llamadas de extorsión al día. En 2010, la cifra se incrementó en más de 40% al alcanzar las 6,400 diarias.

En gran medida, la incapacidad del RENAUT ha sido producto de la idea de que el registro de usuarios de celulares en una gran base de datos nacional garantizaría la ubicación de los responsables de un delito. Una idea errónea fundada sobre el argumento de que los delincuentes utilizarían aparatos de comunicación móvil registrados a su nombre o a nombre de sus cómplices. La realidad es otra.

Tal como se ha señalado en esta misma tribuna, el registro de un teléfono mediante nombre y Clave Única de Registro de Población (CURP) no garantiza la veracidad de los datos y menos aún que en el caso de cometerse un delito realmente se atrape al

culpable; por el contrario, puede culparse a una persona que no lo sea. Asimismo, resulta inoperante la obligación de los concesionarios de verificar la veracidad de la información suministrada pues las compañías operan a través de miles de distribuidores y agentes a los que no puede hacerse responsables de hacerlo.

Por otra parte, no hay incentivos para garantizar que las personas que contratan un servicio de comunicación por celular y que se registran mantengan los mismos datos en un periodo posterior. De tal forma que el RENAUT además de contener registros falsos, también contiene registros desactualizados.

Asimismo, algunos especialistas afirman que la obligación de registrar teléfonos móviles ha generado incentivos para el robo de equipos. Como ya se ha dicho, se calcula que cerca del 40% de los asaltos a transeúntes tiene como objetivo el robo de equipos celulares.

Existen otros datos que hablan por sí mismos de la ineficacia del RENAUT. No debe perderse de vista que cualquier delincuente puede hacer uso de un teléfono comprado en el extranjero con el servicio de "roaming", realizar una llamada con enlace de un equipo de cómputo o comprar un chip en menos de 70 pesos en el mercado informal, ya sea robado o inscrito de forma fraudulenta en el RENAUT, para extorsionar, secuestrar o cometer cualquier otro ilícito.

Un problema adicional es la posibilidad de que la información suministrada por los usuarios pueda ser sustraída de la base de datos y empleada de forma indebida.

Al final, queda claro que el RENAUT se inscribe en una clara tendencia de dejar en manos de los ciudadanos responsabilidades y deberes que corresponden exclusivamente a la autoridad..."

"...El 9 de febrero de 2009 se publicó en el Diario Oficial de la Federación el decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones, con el objetivo fundamental de establecer el Registro Nacional de Usuarios de Telefonía Móvil (RENAUT) a fin de coadyuvar en la prevención, investigación y persecución de delitos como el secuestro y la extorsión, en los que frecuentemente se utilizan teléfonos móviles.

Sin embargo, a casi dos años de la publicación del decreto las reformas no han logrado los resultados esperados. Pero no sólo eso: su diseño inadecuado ha facilitado la comisión de aquellos delitos que se buscó combatir o ha generado lagunas e incentivos para la comisión de conductas como el robo de datos personales.

Las vulnerabilidades del RENAUT fueron visibles desde los primeros días. Incluso, a unas horas de iniciar su operación, aparecieron registros falsos a nombre de personalidades de la historia, la política, los deportes o la farándula. Basta decir que a mediados de 2010 la Comisión Federal de Telecomunicaciones (COFETEL) informó que entre 10 mil y 50 mil registros eran apócrifos. Hace unos meses el presidente de la COFETEL, Mony de Swaan, reconoció que el RENAUT debe revisarse, pues ni siquiera se ha avanzado en la etapa de verificación de la identidad de los usuarios registrados.

Como bien han señalado diversos especialistas, el registro de un teléfono mediante nombre y Clave Única de Registro de Población (CURP) no garantiza la veracidad de los datos y menos aún que en el caso de cometerse un delito realmente se atrape al culpable; por el contrario, puede culparse a una persona que no lo sea.

Por otro lado, no debemos perder de vista que la venta de tarjetas SIM, mejor conocidos como chips telefónicos, en el mercado informal permite a cualquiera tener acceso a una línea de teléfono móvil sin ser responsable de las llamadas que realice. En realidad, cualquier miembro de la delincuencia organizada que requiera un celular para extorsionar, secuestrar o cometer cualquier otro ilícito, sólo tiene que invertir 70 pesos para comprar en el mercado informal un chip, inscrito de forma fraudulenta en el RENAUT, que le permitirá disponer de una línea sin que ninguno de sus datos queden registrados. Si los chips se compran por mayoreo, su precio puede bajar hasta 50 pesos.

Y cuando la delincuencia no tiene acceso a un chip, puede recurrir a métodos tradicionales. Se calcula que cerca del 40% de los asaltos a transeúntes tiene como objetivo el robo de equipos celulares.

Como si todo lo anterior no fuese suficiente, debemos señalar que ha sido ampliamente documentada la comercialización de los datos contenidos en el RENAUT. Tan sólo en el mes de junio de 2010 diversos usuarios de internet ofrecían el padrón completo de usuarios por 500 pesos, con la posibilidad de recibirlo en disco compacto hasta la puerta de la casa.

Un dato final: de acuerdo con cifras de diversas organizaciones civiles, en 2008, antes de la implementación del RENAUT, se registraban cerca de 4,400 llamadas de extorsión al día. En 2010, la cifra se incrementó en más de 40% al alcanzar las 6,400 diarias.

Entonces cabe preguntarse ¿para qué ha servido el RENAUT?...”

301. En esa tesitura, este Tribunal Pleno, con base en experiencias anteriores, valora que no es posible sostener que la creación de este tipo de padrones garantice que efectivamente se vaya a identificar a los responsables de los delitos, experiencias que ilustran, además, que, ante fallas de seguridad, ese tipo de padrones conllevan riesgos importantes para la protección de los datos personales e incluso pueden facilitar la comisión misma de los delitos que pretende combatir.
302. Pero, además, tampoco existen elementos suficientes que nos permitan afirmar de manera categórica que la información que proporciona el PANAUT a las autoridades investigadoras es *mejor o más idónea* para identificar a los presuntos responsables de aquella que pueda obtenerse de la intervención de una comunicación privada.
303. Por el contrario, nada impide pensar que la identificación de dichos agentes pueda realizarse de forma igualmente efectiva a través de la intervención de comunicaciones privadas, pues como se señaló anteriormente, el cúmulo de información y datos generados en los procesos comunicativos puede ser muy vasto, valioso y útil para tal finalidad; nombres, direcciones, parentescos, pseudónimos, actividades, ubicación, son datos que pueden obtenerse a través del uso de estas técnicas y que desde luego, ayudan en gran medida a identificar a los infractores, considerando además, que los concesionarios tienen ya la obligación de conservar el nombre y domicilio del suscriptor al margen del PANAUT, en los términos del artículo 190, fracción II, de la ley impugnada.
304. Finalmente, se estima que esta objeción parte de un enfoque equivocado.
305. En efecto, se ha explicado que la idoneidad de la medida implica reconocer la conexión que en términos de utilidad existe entre la opción adoptada y el fin perseguido. En ese sentido, debe recordarse que el fin legítimo que persigue el PANAUT es colaborar con las autoridades de justicia en relación con la comisión de un delito, especialmente cuando se realiza mediante telefonía celular.
306. Si esta es la finalidad, ¿podría afirmarse que la creación del PANAUT es más idónea que la intervención de comunicaciones para poder satisfacerla? Lo realidad es que no, puesto que ambas herramientas son susceptibles de proporcionar información sumamente valiosa para la investigación, persecución y sanción de este tipo de delitos.
307. Pero aun concediendo que con la creación del PANAUT se permita identificar con mayor facilidad a los posibles responsables de la comisión de estos delitos, ello no conduce a sostener que la medida por tanto es *más idónea* para colaborar con las autoridades de justicia en relación con la comisión de un delito, pues la identificación de los posibles implicados constituye sólo uno de los elementos de aquello que debe investigarse a fin de poder fincar las responsabilidades y establecer las sanciones penales correspondientes, por tanto, contar con esta información no implica por sí mismo que el combate a la delincuencia va a ser más efectivo.
308. En consecuencia, este Tribunal Pleno considera que ambas medidas –intervención de comunicaciones y PANAUT– son igualmente idóneas para colaborar con las autoridades de justicia en relación con la comisión de un delito, pues ambos mecanismos son susceptibles de proporcionar a las autoridades de seguridad y procuración de justicia información útil a fin de investigar las conductas, identificar a los responsables e imponer las sanciones respectivas.
309. No obstante, a pesar de que existe una equivalencia en términos de utilidad entre ambas medidas, debe reconocerse que, en su conjunto, la intervención de comunicaciones privadas **resulta una medida menos restrictiva** de los derechos a la privacidad y protección de datos personales de lo que resulta la creación y regulación del PANAUT.
310. Esto porque, si bien intervenir las comunicaciones privadas de los particulares representa en sí mismo una afectación fuerte en el derecho a la privacidad, lo cierto es que la figura se encuentra revestida de una serie de garantías y salvaguardas que permiten advertir que, en su conjunto, someten a estos derechos a un nivel *más bajo de afectación* de aquella que produce el PANAUT.

311. En primer lugar, porque el acceso del Estado a esta información **no es generalizado**, es decir, no se permite que las autoridades competentes puedan acceder de manera irrestricta a todos los procesos de comunicación que se lleven a cabo a través del uso de telefonía móvil. Por el contrario, de los artículos 292 y 293 del Código Nacional de Procedimientos Penales se puede apreciar que el acceso a dicha información **es limitado**.
312. Tanto en la solicitud de intervención de comunicaciones como en la autorización que en su caso otorgue el juez, debe precisarse: *i)* la persona o personas que serán sujetas a la medida; *ii)* la identificación del lugar o lugares donde se realizará; *iii)* si fuere posible, el tipo de comunicación intervenida; *iv)* su duración; *v)* el proceso que se llevará a cabo; y *vi)* las líneas, número o aparatos que serán intervenidos y en su caso, *vii)* la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realizará la comunicación objeto de intervención.
313. Esto quiere decir que la intervención de las comunicaciones privadas está circunscrita un caso en particular, a una persona o personas en concreto, o a un equipo o línea en específico, por lo que no puede abarcar *a todos los usuarios de telefonía móvil ni a todos los procesos de comunicación*, lo que evita que se instaure un sistema de vigilancia generalizado que, como correctamente lo afirman los accionantes, iría en contra de las bases de una sociedad democrática.
314. Sobre este punto en específico debe advertirse que los *Principios del CJI*, concretamente el *Principio Tres* referido a la *Pertinencia y Necesidad*, establece lo siguiente:
- “Los datos personales deberían ser únicamente los que resulten adecuados, pertinentes y **limitados al mínimo necesario** para las finalidades específicas de su recopilación y tratamiento ulterior”*
315. Al respecto, señala el referido Comité que la pertinencia y la necesidad son principios cruciales de la protección de datos y la privacidad personal. Desde luego, sus requisitos deben evaluarse en relación con el contexto específico en el cual se recopilen y ulteriormente traten los datos. Las consideraciones contextuales incluyen qué datos particulares se recopilan y con qué finalidades.
316. Respecto de la pertinencia, el Comité refiere que este requisito significa que los datos personales requeridos deben guardar una relación razonable con la finalidad para la cual hayan sido recopilados y se tenga la intención de usarlos.
317. Por su parte, explica que la necesidad tiene una doble dimensión. En primer lugar, impone que los datos personales sean tratados solamente de una forma acorde con las finalidades expresas de su recopilación, por ejemplo, cuando sean necesarios para proporcionar el servicio o el producto solicitado por la persona. Pero, además, implica que los recopiladores y encargados de datos deben seguir un criterio de “limitación” o “minimización”, de acuerdo con el cual deben hacer un esfuerzo razonable para cerciorarse de que los datos personales que manejen correspondan al **mínimo necesario** para la consecución de la finalidad expresa.
318. Sobre este punto son coincidentes los *Estándares Iberoamericanos*, pues el Principio 18, denominado Principio de Proporcionalidad, establece que *“el responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.*
319. Estos estándares se encuentran incorporados en nuestro derecho interno por la Ley General de Protección de Datos en Posesión de Sujetos Obligados, pues su artículo 16 establece que el responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.¹⁰⁵ Por su parte, el artículo 25 establece que dicho responsable **sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.**¹⁰⁶ Finalmente, el ya referido artículo 80 establece que la obtención y tratamiento de datos personales por parte de los sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos.¹⁰⁷

¹⁰⁵ Artículo 16. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

¹⁰⁶ Artículo 25. El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

¹⁰⁷ Artículo 80. La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de los sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto. Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en el presente Capítulo.

320. En contraposición a estos estándares, el sistema normativo que crea y regula el PANAUT impone la **recopilación generalizada** de información privada y de datos personales, pues la obligación de entregar esta información recae sobre **todas aquellas personas físicas o morales que sean titulares de una línea de telefonía móvil.**
321. El riesgo de la medida se impone por sí mismo, pues como se explicó, hoy en día la tenencia y el uso de un celular es una práctica muy extendida que tiene una importancia creciente en la vida cotidiana de las personas. Tan es así, que conforme al Banco de Información de Telecomunicaciones (BIT)¹⁰⁸ emitido por el Instituto Federal de Telecomunicaciones, al primer trimestre de dos mil veintiuno, el número de líneas telefónicas móviles existentes era de 123,377,078 (ciento veintitrés millones trescientos setenta y siete setenta y ocho), lo que implica que hasta el año pasado existían **noventa y ocho líneas por cada cien habitantes.**
322. En consecuencia, dada la densidad de líneas de telefonía móvil que hoy en día existe, debe advertirse que el Estado a partir de la creación y regulación del PANAUT, podrá recopilar, administrar, conservar por tiempo indefinido y tener acceso a la información básica privada y más íntima **de casi de toda la población del país.**
323. Sobre este punto, debe resaltarse que la generalización de la medida a tal escala conlleva que la entrega de los datos personales e íntimos de los usuarios de telefonía móvil al Estado, así como su acceso y disponibilidad, no presupone una relación entre dichos datos y una amenaza para la seguridad pública vinculada con la comisión de un delito, pues a pesar de que las personas no se encuentren ni siquiera indirectamente en una situación que pueda dar lugar a acciones penales, de todas maneras deberá entregar su información al Estado.
324. La medida aplica por igual a personas respecto de las que no existen indicios que sugieran que su comportamiento pueda guardar relación, incluso indirecta o remota, con delitos. No se prevé algún tipo de excepción, abarca a cualquier tipo de usuarios sin distinción, incluyendo por ejemplo a menores de edad, como correctamente lo afirman los accionantes.
325. De estos aspectos, es posible concluir que el legislador optó por establecer una medida global y estandarizada, que implica recabar de forma indistinta la información privada e íntima prácticamente toda la población del país y entregársela al Estado, con independencia de que las personas o la información esté relacionada, directa o indirectamente con los hechos delictivos.
326. Para este Tribunal Pleno, este criterio de recopilación y acceso es contrario a los estándares previamente expuestos, pues el principio de necesidad de la información obliga a reconocer que la conservación y al acceso a la información privada y datos personales debe responder a criterios objetivos que permitan advertir una relación entre los datos que sean objeto de tratamiento y el objetivo que se pretende lograr. La recopilación y el acceso a los datos debe responder efectiva y estrictamente a la satisfacción de tales objetivos. En particular, estos criterios deben permitir que pueda delimitarse en la práctica de modo efectivo el alcance de la medida y, en consecuencia, el público afectado.¹⁰⁹
327. En consecuencia, una recopilación que incluya a todos los usuarios de telefonía móvil y cuya entrega se realiza directamente al Estado con independencia de que exista una relación, al menos indirecta, con el fin perseguido, **no puede considerarse limitada a lo estrictamente necesario.** Por el contrario, este requisito de necesidad, en atención al fin legítimo previamente identificado, estaría vinculado con los datos de personas de las que se encuentren relacionadas con la posible comisión de un delito.
328. En contraposición, la intervención de comunicaciones, como quedó expuesto, está circunscrita a casos particulares, a una persona o personas en concreto, o a equipos o líneas en específico y sobre todo, a la existencia de razones y motivos que relacionen a dichas personas o equipos con las conductas que se investigan, por tanto, no implica la intervención de *todas las comunicaciones*, ni incluye *todos los usuarios de telefonía móvil*, lo que evita que se instaure un sistema de vigilancia generalizado.

¹⁰⁸ Consultable en el siguiente link: <https://bit.ift.org.mx/BitWebApp/informacionEstadistica.xhtml>

¹⁰⁹ Sobre este punto resulta sumamente ilustrativa la jurisprudencia emitida por el Tribunal de Justicia de la Unión Europea a partir de diversas resoluciones en las que analizó la compatibilidad entre los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea que protegen la privacidad y los datos personales, frente a diversas directivas que trataban de establecer estándares generales sobre la conservación por parte de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, de determinados datos generados o tratados por dichos proveedores para garantizar que los datos estén disponibles con fines de prevención, investigación, detección y enjuiciamiento de delitos graves.

Véase Digital Rights Ireland y Seitlinger y otros. C-293/12 y C-594/12. Sentencia de 8 de abril de 2014. Tele2 Sverige y Watson y otros. C-203/15 y C-698/15. Sentencia de 21 de diciembre de 2016. Ministerio Fiscal. C-207/16. Sentencia de dos de octubre de dos mil dieciocho. Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL y otros. C-520/18. Sentencia de quince de enero de dos mil veinte. Privacy International y otros. C-623/17. Sentencia de seis de octubre de dos mil veinte.

Desde luego, se reconoce que estas resoluciones no son en sentido alguno vinculantes para esta Corte, no obstante, resultan orientadoras acerca de la perspectiva a partir de la cual el referido Tribunal Europeo afronta una problemática muy similar a la que ahora se analiza.

329. De ahí que resulte medianamente clara la diferencia que sobre este punto existe en el grado de afectación a los derechos de privacidad y protección de datos personales entre un mecanismo y otro.
330. Otro aspecto que debe resaltarse sobre la intervención de las comunicaciones privadas es que la injerencia que provoca en estos derechos **está sujeta a un control judicial**, pues por mandato expreso de la Constitución General y del Código Nacional de Procedimientos Penales, la intervención de comunicaciones debe ser necesariamente autorizada y supervisada por un juez, lo que de entrada imprime una importante salvaguarda para estos derechos.
331. En contraposición, de la regulación del PANAUT **no se advierte que el acceso del Estado a la información privada y los datos personales de los usuarios de telefonía móvil esté sujeto a un control judicial.**¹¹⁰
332. Por el contrario, de las normas que integran el Decreto impugnado se puede apreciar que toda la información que integre el PANAUT va a ser entregada por mandato legal al Estado, a través del Instituto Federal de Telecomunicaciones, pues de conformidad con los artículos 15, fracción XLII Bis, 180 Quintos y 180 Sextus de la Ley Federal de Telecomunicaciones y Radiodifusión, los concesionarios de telecomunicaciones y en su caso, los autorizados, deberán **recabar** la información de los usuarios de telefonía móvil para después **ingresarla** al Padrón Nacional de Usuarios de Telefonía Móvil, el cual será instalado, operado, mantenido y validado por el Instituto Federal de Telecomunicaciones.
333. Esto significa que todos los datos e información que integran el PANAUT estará en manos del Estado de manera automática por efecto de las normas que se combaten, de tal suerte que para otorgar dicho acceso no se requerirá de orden judicial o mecanismo jurídico adicional. En otras palabras, por mandato de ley el Estado **es el poseedor, administrador y operador** de toda esta información privada, datos personales y datos sensibles entregados por todos los usuarios de telefonía móvil, lo que nuevamente imprime un fuerte riesgo a la privacidad e intimidad de las personas.
334. Contrario a esta situación y a fin de establecer salvaguardas suficientes que garanticen que la limitación al derecho a la privacidad y el acceso a los datos personales sea el estrictamente indispensable y necesario en estos supuestos de investigación y persecución de delitos, es que este Tribunal Pleno estima necesario establecer que dicho acceso por un lado, debe estar condicionado a criterios objetivos que permitan definir las circunstancias y los requisitos conforme a los cuales pueda otorgarse y además, salvo en casos de urgencia debidamente justificados, dicho acceso debe estar sujeto a un control previo de un órgano jurisdiccional.
335. En esa tesitura, el hecho de que todos los usuarios de telefonía móvil deban entregar su información privada y datos personales directamente al Estado, tal y como lo establece el Decreto impugnado, resulta claramente incompatible con este parámetro.¹¹¹
336. No pasa inadvertido que el artículo 180 Septimus, último párrafo, de la Ley Federal de Telecomunicaciones establece que las autoridades de seguridad, procuración y administración de justicia que cuenten con la facultad expresa para requerir los datos del PANAUT podrán tener acceso a esta información.
337. Sin embargo, debe reiterarse que esta previsión no regula el acceso del Estado a la información que integra el PANAUT, pues como ha quedado expuesto, dicho acceso ya lo tiene por mandato legal al ser el poseedor, administrador y operador de la misma, de tal suerte que lo único que regula este precepto es **la transferencia** de la información de un órgano del Estado a otro, concretamente del Instituto Federal de Telecomunicaciones a las autoridades procuración y administración de justicia.
338. Sobre este punto cabe destacar que dicha transferencia tampoco se sujeta a un control judicial previo, de hecho, el Decreto combatido ni siquiera precisa qué autoridades, en qué supuestos o bajo qué circunstancias o con arreglo a qué requisitos el Instituto Federal de Telecomunicaciones deberá otorgar

¹¹⁰ Para efectos de claridad en la votación emitida por el Pleno de la Suprema Corte de Justicia de la Nación en las sesiones de los días veinticinco y veintiséis de abril de dos mil veintidós, específicamente, en relación con el voto emitido por la señora Ministra Esquivel Mossa y el señor Ministro Pardo Rebolledo, quienes manifestaron apartarse del párrafo 310 del proyecto de sentencia sometido a consideración del tribunal Pleno, se informa que, derivado de las modificaciones aceptadas en dichas sesiones, tal párrafo pasó a ser el número 331 en el presente engrose.

¹¹¹ Para efectos de claridad en la votación emitida por el Pleno de la Suprema Corte de Justicia de la Nación en las sesiones de los días veinticinco y veintiséis de abril de dos mil veintidós, específicamente, en relación con el voto emitido por la señora Ministra Esquivel Mossa y el señor Ministro Pardo Rebolledo, quienes manifestaron apartarse de los párrafos 313 y 314 del proyecto de sentencia sometido a consideración del tribunal Pleno, se informa que, derivado de las modificaciones aceptadas en dichas sesiones, tales párrafos pasaron a ser los números 334 y 335 en el presente engrose.

el acceso a esta información a las autoridades de investigación y procuración de justicia, ni tampoco si en determinados supuestos y en cuáles, podrá negarse a dicha solicitud, aspectos que en opinión de este Tribunal Pleno, era necesario que estuvieran contemplados en una ley y no en disposiciones administrativas.¹¹²

339. Nuevamente, derivado de este aspecto relativo al **control previo**, debe concluirse que el riesgo que genera el PANAUT en los derechos a la privacidad y protección de datos personales de los usuarios de telefonía móvil es mayor de aquel que plantea la intervención de comunicaciones privadas.
340. Otro elemento que resulta de la mayor relevancia para efectos de este estudio comparativo es que la intervención de las comunicaciones privadas **es temporal**. En efecto, el artículo 292 del Código Nacional de Procedimientos establece que el plazo de la intervención incluyendo prórrogas, no podrá exceder de seis meses, por lo que transcurrido dicho plazo sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen. Por su parte, el artículo 300 de dicha legislación penal establece entre otras cosas, que los registros de las intervenciones serán destruidos una vez que se decreta el archivo definitivo, el sobreseimiento o la absolución del imputado.
341. A diferencia de lo anterior, de los diversos preceptos que integran el Decreto que crea y regula el PANAUT no se advierte la existencia de alguna previsión legal que sujete a alguna temporalidad la conservación de la información privada y datos personales de los usuarios de telefonía móvil, lo que permite inferir que la afectación a estos derechos tiene una condición permanente.
342. Sobre este punto, conviene referir nuevamente a los *Principios del CJI*, pues el *Principio Cuarto* que habla del *Tratamiento y Conservación Limitados*, establece lo siguiente:
- “Los datos personales deberían ser tratados y conservados solamente de manera legítima no incompatible con las finalidades para las cuales se recopilaron. Su conservación no debería exceder del tiempo necesario para cumplir dichas finalidades, de conformidad con la legislación nacional correspondiente.”*
343. Por su parte, los *Estándares Iberoamericanos* prevén el siguiente texto:
- “19. Principio de calidad**
- 19.1. *El responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.*
- 19.2. **Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.**
- 19.3. *En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos.*
- 19.4. **Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas relacionadas con exigencias legales aplicables al responsable. No obstante, la legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer excepciones respecto al plazo de conservación de los datos personales, con pleno respeto a los derechos y garantías del titular.”**
344. Al respecto, el Comité Jurídico Interamericano ha señalado que los datos personales deben conservarse de forma que se permita la identificación de sus titulares **únicamente durante el tiempo que sea necesarios para las finalidades del tratamiento**. Sostiene que la realidad de la tecnología moderna exige una limitación general sobre este aspecto, pues la conservación innecesaria y excesiva de esta información tiene evidentes implicaciones negativas para la privacidad y la protección de los datos personales.

¹¹² Para efectos de claridad en la votación emitida por el Pleno de la Suprema Corte de Justicia de la Nación en las sesiones de los días veinticinco y veintiséis de abril de dos mil veintidós, específicamente, en relación con el voto emitido por la señora Ministra Esquivel Mossa y el señor Ministro Pardo Rebolledo, quienes manifestaron apartarse del párrafo 317 del proyecto de sentencia sometido a consideración del tribunal Pleno, se informa que, derivado de las modificaciones aceptadas en dichas sesiones, tal párrafo pasó a ser el número 338 en el presente engrose.

345. Por tanto, los responsables deben disponer de los datos de una manera segura y definitiva a través, por ejemplo, de eliminar sus archivos, registros, bases de datos, expedientes o sistemas de información, o bien someterlos a un proceso de *anonimización*, cuando ya no se necesiten para su fin original o tal como se disponga en la legislación nacional.
346. Se precisa que los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines archivísticos, de investigación científica e histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas para proteger los derechos y libertades del titular.
347. Debe señalarse, que este estándar internacional se encuentra incorporado en nuestro derecho interno, pues los artículos 23 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 11 y 13 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares establecen que los plazos de conservación de los datos personales no deben exceder aquellos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, de tal suerte que concluido y una vez que los datos hayan dejado de ser necesarios, deberán ser suprimidos.¹¹³
348. A la luz de esos estándares, como ya se mencionó, debe advertirse que el sistema normativo que crea y regula el PANAUT **no establece una temporalidad** a la cual estará sujeta la conservación de los datos personales de los usuarios de telefonía móvil, lo que permite inferir entonces que dicha conservación será por tiempo indefinido, aspecto que resulta contrario a los estándares nacionales e internacionales previamente expuestos.
349. No se deja de advertir que, acorde con tales parámetros, la temporalidad de la conservación de los datos puede no estar determinada por un plazo en específico, sino por la utilidad que la información represente para la satisfacción de una determinada finalidad. Sin embargo, aun reconociendo este aspecto, lo cierto es que la conservación de la información debe continuar estando sujeta a una temporalidad, la cual puede no estar determinada, pero ser determinable, sin que dicho grado de indeterminación pueda traducirse en una conservación de datos por tiempo indefinido.
350. Recordemos que el Comité es claro en establecer que la realidad de la tecnología moderna exige una limitación general por cuanto hace a la conservación de los datos personales, de ahí que dicha conservación **debe ser necesariamente temporal**, pues la conservación innecesaria y excesiva compromete de manera importante la protección de la privacidad y los datos personales.
351. En ese sentido, no puede sostenerse que la temporalidad de la conservación de la información que integra el PANAUT está implícita, en tanto deba entenderse que los datos se conservarán mientras sean útiles y necesarios para el combate de los delitos cometidos mediante el uso de dispositivos móviles.
352. Esto porque, dada la naturaleza de esta finalidad, su satisfacción en la realidad no estaría sujeta a una temporalidad, o ¿cuándo puede considerarse que esta información ha perdido su utilidad para efecto de contribuir en la investigación y persecución de delitos cometidos mediante el uso de teléfonos celulares? Cuando ya no se cometan delitos a través del uso de un celular, o bien, cuando se tenga la certeza de que el titular de los datos ya no cometerá un delito a través de estos dispositivos. Ambos supuestos se tornan irrazonables, de ahí que en opinión de este Tribunal Pleno no se puede adoptar

¹¹³ LGPDPPSO

Artículo 23. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

LFPDPPP

Artículo 11.- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.

El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

Artículo 12.- El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.

Artículo 13.- El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el período de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

este criterio, pues ello implicaría defraudar la razón de ser de estos estándares que buscan fijar siempre un límite temporal a la conservación de información privada y datos personales. En consecuencia, no es posible que a través de esta interpretación se autorice la conservación por tiempo indefinido de información privada por parte del Estado.

353. Así, a la luz de las consideraciones expuestas anteriormente, debe reconocerse que la intervención de comunicaciones privadas es una herramienta de investigación que resulta igualmente *idónea* para colaborar con las autoridades de justicia en relación con la comisión de un delito que se cometa mediante el uso de dispositivos de telefonía móvil, puesto que es susceptible de proporcionar información valiosa y útil a las autoridades de procuración y administración de justicia a fin de investigar las conductas, identificar a los sujetos activos del delito, así como fincar las responsabilidades penales correspondientes.
354. Sin embargo, esta medida resulta menos restrictiva de los derechos a la privacidad y protección de datos personales en comparación con la que genera el PANAUT, pues la restricción que produce en estos derechos no es generalizada sino concreta y determinada, es temporal y no permanente, y, sobre todo, está sujeta a un control judicial.
355. ***Geolocalización y entrega de datos conservados por los concesionarios de telecomunicaciones o autorizados.*** El artículo 190, fracciones I y II, de la Ley Federal de Telecomunicaciones establece la obligación a cargo los concesionarios de telecomunicaciones o autorizados de conservar un registro y control de las comunicaciones realizadas desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, **que permita identificar con precisión**, entre otros, los siguientes datos: *i)* nombre, denominación social y domicilio del suscriptor; *ii)* tipo de comunicación; *iii)* datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil, como son número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago; *iv)* datos necesarios para determinar la hora, fecha y duración de la comunicación; así como *v)* la ubicación digital del posicionamiento geográfico de las líneas telefónicas.
356. De dicho precepto se puede apreciar que los concesionarios de telecomunicaciones ya estaban obligados a generar una base de datos sobre las comunicaciones realizadas a través del uso de dispositivos móviles, precisamente con la finalidad de contribuir con las autoridades de seguridad y procuración de justicia en el combate a la delincuencia, ello a través de la identificación y ubicación de las líneas utilizadas para la comisión de los ilícitos, incluidos el nombre y domicilio del titular de la línea, en cualquiera de sus modalidades de contratación.
357. En tesis, el artículo 303 del Código Nacional de Procedimientos Penales establece que, cuando se estime necesario para la investigación, se podrá solicitar al juez de control que ordene a los concesionarios de telecomunicaciones, autorizados o proveedores de servicios de aplicaciones y contenidos proporcionar con la oportunidad y suficiencia necesaria a la autoridad investigadora la localización geográfica en tiempo real o entrega de los datos conservados de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan.
358. Inclusive se establece que excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador podrá ordenar directamente la entrega de esta información y una vez que este requerimiento haya sido cumplimentado, dichas autoridades deberán informar al Juez correspondiente a fin de que revise dicha actuación.
359. De estos elementos, es posible apreciar que la Ley Federal de Telecomunicaciones y Radiodifusión y el Código Nacional de Procedimientos Penales prevén una figura que permite a las autoridades encargadas de la investigación y persecución de los delitos, acceder a diversa información relacionada con **el uso de una línea de telefonía móvil**, como el nombre y domicilio del suscriptor, los datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil, número de destino, modalidad de líneas con contrato o plan tarifario, la modalidad de líneas de prepago; los datos necesarios para determinar la hora, fecha y duración de la comunicación; así como la ubicación digital del posicionamiento geográfico de las líneas telefónicas.¹¹⁴
360. La pregunta que surge es: ¿este mecanismo es *igualmente idóneo* en relación con el PANAUT para colaborar con las autoridades de justicia, en relación con la comisión de delitos mediante el uso de dispositivos de telefonía móvil?

¹¹⁴ Sobre el particular, resulta de utilidad consultar los "Lineamientos de Colaboración en Materia de Seguridad y Justicia" emitidos por el Instituto Federal de Telecomunicaciones.

361. Para este Tribunal Pleno la respuesta es afirmativa. Primero porque, al igual que el PANAUT, constituye una base de datos relacionada con el uso de líneas de telefonía móvil que tiene por objeto proporcionar información y datos a las autoridades de investigación y procuración de justicia sobre el uso de un determinado dispositivo móvil vinculado con comisión de un delito, la cual podría ser útil y valiosa para la investigación de este tipo de conductas, la identificación de los posibles responsables y su domicilio, así como el establecimiento de las sanciones respectivas, de ahí la relación de instrumentalidad que existe entre la medida y el fin perseguido.
362. En ese sentido, debe reconocerse que la ubicación en tiempo real de un equipo de telefonía móvil, el propio nombre y domicilio del suscriptor, el origen o destino de la comunicación, fecha y hora de la primera activación, el lugar de la compra del dispositivo de prepago o tarjeta SIM o los datos del distribuidor al que fueron entregados tales dispositivos, desde luego que pueden abonar, contribuir y encaminar la investigación hacia la identificación de las personas que utilicen o detentan la posesión de los aparatos y por lo tanto su probable participación en los hechos investigados. Hoy en día resulta innegable la estrecha relación que existe entre un equipo móvil y la persona.
363. Sobre este punto, podría pensarse que el PANAUT, por el tipo de información que lo integra, constituye una herramienta *más idónea* para identificar a quienes cometan delitos a través del uso de un dispositivo móvil. Sin embargo, la realidad es que esto resulta una mera suposición, pues, en primer lugar, nada garantiza que el PANAUT sea eficaz para identificar a los posibles responsables, por el contrario, experiencias pasadas indican que la delincuencia difícilmente utilizará para fines delictivos teléfonos que se encuentren previamente registrados y por el contrario ante fallas de seguridad, ese tipo de padrones conllevan riesgos importantes para la protección de los datos personales e incluso pueden facilitar la comisión misma de los delitos que pretende combatir.
364. Además, tampoco es posible afirmar de manera categórica que la información que proporciona el PANAUT es *mejor o más idónea* en todos los casos para identificar a los presuntos responsables del delito. Como se indicó, información como la ubicación en tiempo real de un equipo de telefonía móvil, el propio nombre y domicilio del suscriptor, así como el origen, destino, duración y demás datos de la comunicación por supuesto que pueden resultar útiles y valiosos para efecto de identificar a los presuntos responsables, sus actividades o relaciones sociales.
365. Pero aun suponiendo que el PANAUT fuera una herramienta que facilita en mayor medida la identificación de los presuntos responsables de un delito, lo cierto es que este aspecto no conduce a sostener necesariamente que la medida es más idónea para colaborar con las autoridades de justicia en relación con la comisión de un delito, pues dicha identificación constituye sólo uno de los elementos de aquello que debe investigarse a fin de poder fincar las responsabilidades y establecer las sanciones penales correspondientes, por lo tanto, no es posible sostener que contar con la base de datos que conforman el PANAUT implica por sí mismo que el combate a la delincuencia va a ser más efectivo.
366. Por tanto, debe de concluirse que ambos mecanismos –PANAUT y la geolocalización y entrega de los datos conservados por los concesionarios de telecomunicaciones– constituyen herramientas igualmente idóneas para colaborar con las autoridades de justicia en relación con la comisión de un delito cometido mediante el uso de un dispositivo móvil.
367. Sin embargo, a pesar de la equivalencia en la utilidad de estas dos figuras, la realidad es que, a juicio de este Tribunal Pleno, la entrega de la geolocalización y demás datos conservados, analizada en su conjunto, constituye una medida menos restrictiva de los derechos a la privacidad y protección de datos personales.
368. De entrada, porque, derivado del tipo de información que se **recopila y almacena**, el grado de injerencia en los derechos a la privacidad y protección de datos personales no es el mismo. Básicamente, porque no es lo mismo que se recopilen y conserven los datos relacionados con el origen y destino de una llamada a que se recopilen y almacenen los datos biométricos de una persona. Desde luego, ambos tipos de información están tutelados por los derechos a la privacidad y la protección de datos personales,¹¹⁵ y en esa medida su conocimiento por parte de terceros, ya sea el Estado o cualquier particular, constituye de entrada una afectación importante a su ámbito de protección. Sin embargo, derivado de la naturaleza de la información y su vinculación más estrecha con la persona, debe reconocerse que este grado de afectación no es el mismo.
369. Por otro lado, esta medida, a diferencia del PANAUT, tampoco implica **la entrega masiva y generalizada** de información privada y datos personales al Estado. Por el contrario, acorde con el artículo 303 del Código Nacional de Procedimientos Penales el acceso a esta información debe estar referida a personas concretas o a dispositivos móviles específicos.

¹¹⁵ Véase CIDH, Caso Escher y otros vs Brasil, sentencia de 6 de julio de 2009, párr. 114 y 115

370. En efecto, conforme a dicho precepto el acceso a esta información supone la identificación de los equipos de comunicación móvil relacionados con los hechos que se investigan, o bien de las personas que se estiman involucradas, la existencia de motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, duración y en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas, números o aparatos que serán objeto de la medida.
371. De lo anterior se desprende que el acceso del Estado a la información privada y datos personales de los usuarios de telefonía móvil es restringido, pues sólo se permite en ciertos supuestos acotados a personas en específico o equipos móviles en concreto, y, además, exige la existencia de razones y motivos que vinculen a las personas o equipos con los hechos investigados.
372. En esa misma línea, debe decirse que el acceso a esta información por parte de las autoridades de investigación y procuración de justicia está condicionado a **la autorización de un juez**. Incluso en los casos de excepción en los que la propia autoridad investigadora puede solicitar directamente el acceso a esta información, la norma establece que una vez obtenida, el juez debe de ratificar esta actuación y en caso de que no sea así, la información obtenida no podrá ser incorporada al proceso penal por lo que deberá ser destruida.¹¹⁶
373. Finalmente, debe advertirse que, a diferencia del PANAUT, la injerencia que esta medida impone a los derechos a la privacidad y protección de datos personales también es **temporal**, pues, por un lado, tanto la entrega de la geolocalización de los equipos de telefonía móvil como de los demás datos conservados están sujetos a un tiempo determinado;¹¹⁷ pero, además, el tiempo de conservación también está limitado, pues conforme al artículo 190, fracción II, de la Ley Federal de Telecomunicaciones, los concesionarios deberán conservar los datos de las comunicaciones durante los primeros doce meses de producida la comunicación en sistemas que permitan su consulta y entrega en tiempo real. Concluido dicho plazo, deberán conservar tales datos por doce meses adicionales en sistemas de almacenamiento electrónico. Esto quiere decir que, al cabo de tales plazos, los concesionarios ya no tienen la obligación de conservar estos datos para efecto de poder proporcionárselos al Estado a fin de colaborar con las autoridades de seguridad y procuración de justicia.
374. En virtud de estas razones es que se concluye que la medida prevista por los artículos 190, fracciones I y II, de la Ley Federal de Telecomunicaciones y 303 del Código Nacional de Procedimientos penales resulta igualmente *idónea* para colaborar con las autoridades de justicia en relación con la comisión de un delito que se comete mediante el uso de dispositivos de telefonía móvil, puesto que dicha medida es susceptible de proporcionar información valiosa y útil a las autoridades de procuración y administración de justicia a fin de investigar las conductas, identificar a los sujetos activos del delito, así como fincar las responsabilidades penales correspondientes.
375. Sin embargo, dicha medida resulta menos restrictiva de los derechos a la privacidad y protección de datos personales en comparación con el PANAUT, pues la restricción que produce en estos derechos no es generalizada sino concreta y determinada; es temporal y no permanente, y, sobre todo, está sujeta a un control judicial.¹¹⁸
376. **Medidas complementarias.** Ahora bien, a estas medidas anteriormente descritas habría que agregarse las previstas en las fracciones VIII y XII del artículo 190 de la Ley Federal de Telecomunicaciones.
377. La primera se refiere a la obligación de los concesionarios de telecomunicaciones y autorizados para colaborar con las autoridades competentes a fin de que en el ámbito técnico operativo se cancelen o anulen de manera permanente las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen dentro del perímetro de centros de readaptación social, establecimientos penitenciarios o centro de internamiento para menores, federales o de las entidades federativas, la cual abarcará sobre todas las bandas de frecuencia que se utilicen para la recepción en los equipos terminales de comunicación.

¹¹⁶ Para efectos de claridad en la votación emitida por el Pleno de la Suprema Corte de Justicia de la Nación en las sesiones de los días veinticinco y veintiséis de abril de dos mil veintidós, específicamente, en relación con el voto emitido por la señora Ministra Esquivel Mossa y el señor Ministro Pardo Rebolledo, quienes manifestaron apartarse del párrafo 351 del proyecto de sentencia sometido a consideración del tribunal Pleno, se informa que, derivado de las modificaciones aceptadas en dichas sesiones, tal párrafo pasó a ser el número 372 en el presente engrose.

¹¹⁷ Véanse los "*Lineamientos de Colaboración en Materia de Seguridad y Justicia*" emitidos por el Instituto Federal de Telecomunicaciones.

¹¹⁸ Sobre esta medida en específico cabe precisar que esta Suprema Corte de Justicia ya ha tenido oportunidad de pronunciarse acerca de su validez constitucional al resolver la Acción de Inconstitucionalidad 32/2012, así como los Amparos en Revisión 937/2015, 964/2015, 1311/2015 y 264/2016. Sin embargo, debe advertirse que la solución de tales precedentes no puede trasladarse en automático al presente asunto, pues han quedado señaladas las diferencias sustanciales entre esta figura y el PANAUT. No obstante, la presente resolución recoge algunos razonamientos que resultan compatibles y que abonan en la construcción de la solución adoptada.

378. Esta medida resulta importante y útil ya que en los propios *“Lineamientos de Colaboración entre Autoridades Penitenciarias y los Concesionarios de Servicios de Telecomunicaciones y Bases Técnicas para la Instalación y Operación de Sistemas de Inhibición”* emitidos por el Instituto Federal de Telecomunicaciones, se reconoce expresamente que en nuestro país, desde el interior de los centros penitenciarios y en coordinación con bandas delictivas en libertad, se llevan a cabo delitos de extorsión con amenazas de secuestro o de muerte, y fraudes telefónicos contra la sociedad; además que dentro del ambiente penitenciario se cometen acciones de amenaza a familiares de internos, intimidación de testigos, custodios y personal penitenciario; se toman fotografías de las instalaciones y del personal de seguridad para coordinar ejecuciones, evasiones y motines, entre otro tipo de acciones que comprometen la seguridad del lugar y la integridad de las personas.
379. De ahí que la implementación de esta medida pueda contribuir en gran medida a colaborar con las autoridades de justicia en relación con la comisión de delitos, especialmente de los cometidos mediante telefonía celular, la cual, además, es menos restrictiva de los derechos humanos analizados en este asunto, pues de entrada no exige la entrega de la información privada y datos personales de los usuarios de telefonía móvil.
380. Finalmente, la fracción XII establece que los concesionarios y autorizados realizarán bajo la coordinación del Instituto Federal de Telecomunicaciones los estudios e investigaciones que tengan por objeto el desarrollo de soluciones tecnológicas que permitan inhibir y combatir la utilización de equipos de telecomunicaciones para la comisión de delitos o actualizaciones de riesgos o amenazas a la seguridad nacional.
381. Expuesto este conjunto de medidas ya existentes en nuestro ordenamiento jurídico, debe volverse al análisis de la prueba de proporcionalidad.
382. Se ha explicado que esta tercera grada de la prueba obliga a analizar si existen otras medidas o mecanismos que resulten igualmente idóneos para lograr los fines que persigue la medida legislativa adoptada y, en segundo lugar, determinar si estas alternativas intervienen con menor intensidad el derecho fundamental afectado. Así, de encontrarse alguna medida alternativa que sea igualmente idónea para proteger el fin constitucional y que a su vez intervenga con menor intensidad al derecho, deberá concluirse que la medida elegida por el legislador es inconstitucional.
383. Bajo esta metodología es claro que el Decreto por virtud del cual se crea y regula el PANAUT **no supera esta tercera grada de la prueba.**
384. Esto porque ha quedado demostrado que la Ley Federal de Telecomunicaciones y Radiodifusión y el Código Nacional de Procedimientos Penales establecen una serie de mecanismos que resultan igualmente idóneos para satisfacer la finalidad que se propone la medida legislativa analizada, pues al permitir que bajo ciertas condiciones y requisitos se puedan intervenir las comunicaciones privadas, se pueda tener acceso a la geolocalización en tiempo real de un equipo de telefonía móvil, o bien, se entreguen los demás datos de las comunicaciones, incluidos nombre y domicilio del suscriptor, se proporciona a las autoridades de seguridad y procuración de justicia información y datos que pueden resultar sumamente útiles y valiosos para efecto de investigar las conductas delictivas, identificar a los posibles responsables e imponer las sanciones penales que correspondan.
385. Lo anterior significa que estas medidas alternativas resultan igualmente idóneas para colaborar con las autoridades de justicia en relación con la comisión de delitos, especialmente de los cometidos mediante el uso de telefonía celular.
386. No obstante, como se explicó anteriormente, estos mecanismos son menos restrictivos de los derechos a la privacidad y protección de datos personales. Primeramente, porque el acceso a la información que derivan de estas herramientas alternativas está condicionado a la existencia de una **autorización judicial**, lo que de entrada permite una mayor protección de los derechos en juego, pues se garantiza de una mejor manera que estas intervenciones en los derechos fundamentales no se realicen de manera arbitraria e indiscriminada, sino, por el contrario, se encuentren debidamente justificadas y sean resultado de un uso razonable de las facultades investigadoras de la autoridad.
387. Pero, además, el uso e implementación de estas medidas **no entraña el acceso generalizado del Estado a la información privada, personal y sensible de todos los usuarios de telefonía móvil**, lo que en sí mismo genera un grave riesgo en la efectiva protección de estos derechos humanos. Por el contrario, reconociendo que la información que se compromete es por naturaleza sumamente delicada, se busca garantizar que el objeto de la intervención esté perfectamente delimitado y sea concreto en cuanto a las personas, equipos, tiempos y motivos. Así, la forma en la que se configuran estas medidas busca evitar la existencia de **pesquisas generalizadas o peor aún, de sistemas de vigilancia generalizados.**

388. Finalmente, todos estos mecanismos alternativos generan una afectación temporal a los derechos humanos en juego, pues la intromisión que generan en los derechos fundamentales está sujeta a condiciones de tipo temporal, a diferencia de la regulación del PANAUT, la cual no establece por cuanto tiempo el Estado podrá conservar la información privada y los datos personales de los usuarios.
389. En consecuencia, para este Tribunal Pleno es claro que el ordenamiento jurídico mexicano ya preveía una serie de medidas y mecanismos que resultan **igualmente idóneos** para colaborar con las autoridades de justicia en relación con la comisión de delitos, especialmente de los cometidos mediante telefonía celular, **pero que resultan menos restrictivas de los derechos a la privacidad y protección de datos personales, en comparación con el PANAUT.**
390. En ese sentido y a fin de hacer aún más clara esta conclusión, cabe preguntarse: ¿realmente resultaba **necesario** para combatir la delincuencia el recopilar de forma generalizada, conservar por tiempo indefinido y entregar al Estado la información privada y los datos personales de todos los titulares, personas físicas y morales, de una línea de telefonía móvil? ¿Realmente era necesaria esta medida tomando en cuenta que ya existen otras herramientas tecnológicas que proporcionan a las autoridades de seguridad y procuración de justicia información igual de valiosa y útil para la investigación, persecución y sanción de los delitos que se cometan a través del uso de un celular?
391. Para este Tribunal Pleno la respuesta es clara, el PANAUT no resulta una medida legislativa **necesaria** para una sociedad democrática, pues no mantiene un equilibrio entre la necesidad de los datos en circunstancias limitadas y el debido respeto al derecho de privacidad de las personas, además de no encontrar justificación, pues la Ley Federal de Telecomunicaciones y el Código Nacional de Procedimientos Penales ya prevén una serie de mecanismos igualmente idóneos para colaborar con las autoridades de justicia en relación con la comisión de delitos, especialmente de los cometidos mediante telefonía celular, pero que resultan menos restrictivas de los derechos a la privacidad y protección de datos personales.
392. De ahí que deba concluirse que el Decreto impugnado **no supera esta tercera grada del test de proporcionalidad al no ser una medida necesaria para una sociedad democrática.**
- b) Test estricto sobre la afectación a los derechos a la privacidad y protección de datos personales**
393. Como se indicó en apartados precedentes, para analizar la validez del Decreto impugnado resultaba necesario distinguir entre la afectación que sufren los derechos a la privacidad y protección de datos personales, de la afectación que sufren los derechos a la intimidad y protección de los datos sensibles.
394. Lo anterior porque la intimidad constituye un **núcleo protegido con mayor celo y fuerza**, pues dada su estrecha vinculación con los aspectos más íntimos de la persona, exige una protección especial y reforzada, ya que su conocimiento por parte de terceros, coloca a su titular en una situación de extrema vulnerabilidad al hacerlo objeto de conductas discriminatorias susceptibles de ocasionar graves perjuicios en su esfera y poniendo en riesgo los valores más importantes de su individualidad.
395. Es por esto que las potenciales agresiones a la intimidad han sido reconocidas como de una enorme relevancia no solo desde el punto de vista individual sino también colectivo, pues este ámbito dota de las condiciones adecuadas para que las personas pueda desplegar adecuadamente su individualidad, autonomía y libertad, de ahí que su protección tenga una importante función para el desarrollo de sociedades democráticas, en tanto se erige como presupuesto indispensable para el ejercicio del resto de los derechos humanos.
396. En consecuencia, dado que los efectos del Decreto repercuten sobre derechos fundamentales especialmente sensibles que exigen una tutela reforzada, es que en el caso la afectación a los derechos a la intimidad y protección de datos sensibles debe analizarse a la luz de un **escrutinio estricto** a fin de verificar que la medida legislativa, esto es, la creación y regulación del PANAUT tenga una justificación robusta.
397. En esa tesitura, acorde con lo que se expuso en relación con este tipo de escrutinio, lo que procedería es analizar si el sistema normativo que crea y regula el PANAUT, el cual permite al Estado recopilar, administrar, conservar por tiempo indeterminado y tener acceso a la información íntima y los datos sensibles de toda aquella persona física y/o moral que sea titular de una línea telefónica (i) persigue un fin constitucionalmente imperioso; (ii) está estrechamente vinculada con dicha finalidad y (iii) es la medida menos restrictiva posible.
398. No obstante, este Tribunal Pleno advierte que en este punto ya no es necesario agotar toda esa metodología, pues la conclusión de este apartado se deriva lógicamente de la conclusión a la que ya se llegó en el apartado anterior.

399. Esto porque, si la afectación que el Decreto impugnado genera en los derechos a la privacidad y protección de datos personales no resulta razonable a la luz de la prueba **ordinaria** de proporcionalidad, por mayoría de razón, la afectación a los derechos a la intimidad y protección de datos sensibles, que requieren de una protección reforzada, tampoco puede serlo.
400. Sobre este punto, debe precisarse que el Decreto que crea y regula el PANAUT establece un mismo régimen normativo tanto para la información privada y datos personales, como para la información íntima y datos sensibles, es decir ambos niveles de la privacidad de la persona están siendo afectados por el mismo sistema normativo.
401. En consecuencia, si la afectación que este sistema impone al ámbito “ordinario” de la privacidad no resulta razonable, toda vez que no es capaz de superar una prueba ordinaria de proporcionalidad, por mayoría de razón, no puede estimarse razonable la afectación que ese mismo sistema genera en el núcleo protegido con mayor celo y fuerza de la privacidad, pues claramente no va a superar una prueba cuyas gradas exigen un análisis aún más estricto y que requieren de una justificación aún más robusta.
402. Por tanto, este Tribunal Pleno concluye que la afectación a los derechos a la intimidad y protección de datos sensible que genera el Decreto por virtud del cual se crea y regula el PANAUT no es susceptible de superar un escrutinio estricto de proporcionalidad.

C. Conclusión

403. En función de todo lo expuesto en los párrafos anteriores, debe declararse la invalidez del sistema normativo impugnado, toda vez que la creación del Padrón Nacional de Usuarios de Telefonía Móvil genera una afectación a los derechos a la privacidad, intimidad y protección de datos personales que **no resulta razonable**, ya que no supera la prueba de proporcionalidad.
404. Sobre este punto conviene agregar algunos aspectos adicionales.
405. El primero es que del análisis de los preceptos que conforman el Decreto impugnado no se advierte la previsión de salvaguardas o mecanismos de protección **específicos** sobre esta base de datos a fin de que no se vulnere ni se haga mal uso de la información privada y los datos personales entregados por los usuarios de telefonía móvil al Estado.
406. Al respecto, los *Principio Cinco* y *Seis* del CJI, relativos a la *Confidencialidad y Seguridad de los Datos*, establecen lo siguiente:

“Principio Cinco: Confidencialidad

Los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley.”

“Principio Seis: Seguridad de los Datos

La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aún cuando éstos ocurran de manera accidental. Dichas salvaguardias deberían ser objeto de auditoría y actualización permanente.”

407. El referido Comité explica que el Principio Cinco deriva del deber básico del responsable de mantener la “confidencialidad” de los datos personales en un entorno seguro y controlado. Este aspecto viene complementado por el Principio Seis, de acuerdo con el cual los responsables de los datos deben establecer y mantener las medidas de carácter administrativo y técnico que sean necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que obren en su poder o bajo su custodia, así como cerciorarse de que tales datos no sean tratados ni divulgados excepto con el consentimiento de la persona o autoridad legítima, ni sean accidentalmente perdidos, destruidos o dañados.
408. Se precisa que la índole de las salvaguardas implementadas podría variar según la sensibilidad de los datos en cuestión. Evidentemente, los datos sensibles requieren un nivel más alto de protección, a la luz de riesgos, como, por ejemplo, la usurpación de la identidad, pérdidas económicas, efectos negativos en la calificación crediticia, daños a bienes y pérdida del empleo o de oportunidades comerciales o profesionales, la vulneración de la intimidad sexual o actos de violencia de género digital.

409. No obstante, se aclara que, en el contexto moderno, es técnicamente imposible garantizar la privacidad absoluta y la protección completa de los datos personales, puesto que el esfuerzo necesario para lograrlo impondría barreras indeseables y costos inaceptables. Asimismo, es posible que en distintos contextos se requieran soluciones y niveles de salvaguardias diferentes. Por consiguiente, este Principio requiere una valoración razonada e informada y no necesariamente se vulneraría cada vez que un responsable de datos experimente un acceso no autorizado, pérdida, destrucción, daño, uso, modificación o divulgación de los datos personales en su poder, siempre y cuando las medidas y salvaguardias implementadas hayan sido “razonables y adecuadas”.
410. La determinación sobre la razonabilidad y adecuación de las salvaguardias debe basarse en métodos y técnicas de seguridad de los datos consistentes con las buenas prácticas comúnmente aceptadas, al igual que en factores como: i) la evolución constante de las amenazas a la privacidad, especialmente las cibernéticas; ii) los métodos y técnicas más avanzados que estén en uso en el ámbito de la seguridad de los datos, iii) el contexto de la situación general, y iv) la proporcionalidad y necesidad de las medidas tomadas. En ese sentido, las medidas tomadas deberían revisarse, evaluarse, auditarse, actualizarse y mejorarse periódicamente.¹¹⁹
411. Cabe precisar, nuevamente, que estos estándares internacionales han sido incorporados a nuestro derecho interno por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, pues los artículos 31 a 42 establecen una serie de lineamientos que deben cumplir los sujetos responsables de la protección de los datos.
412. Por ejemplo, el artículo 31 establece que el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
413. Por su parte, el artículo 32 señala que las medidas de seguridad deberán considerar: i) el riesgo inherente a los datos personales tratados; ii) la sensibilidad de dichos datos; iii) el desarrollo tecnológico; iv) las posibles consecuencias de una vulneración para sus titulares; v) las vulneraciones previas; vi) el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, entre otros aspectos.
414. Bajo estos parámetros debe reconocerse que el Decreto impugnado **no establece** ningún tipo de salvaguarda, mecanismo de protección o bien, estándares mínimos que deban satisfacerse a fin de proteger de manera efectiva este banco de información privada, datos personales y sensibles de los usuarios de telefonía móvil.
415. En esa tesitura, para este Tribunal Pleno, la magnitud de lo que implica que todos los usuarios de telefonía móvil entreguen su información privada y sus datos personales incluyendo los sensibles, exigía razonablemente el establecimiento de mecanismos específicos que permitieran garantizar una protección eficaz de los datos conservados contra los riesgos de abuso y contra todo acceso ilícito a esos datos. Habida cuenta de la cantidad de datos conservados, del carácter sensible de esos datos y del riesgo de acceso ilícito a éstos, resultaba necesario garantizar la plena integridad y confidencialidad de esos datos, un nivel particularmente elevado de protección y de seguridad mediante medidas técnicas y de gestión adecuadas. Aspectos que era necesario que estuvieran contemplados en una ley y no en disposiciones administrativas.

¹¹⁹ En el mismo sentido se pronuncia el Principio 21 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

21. Principio de seguridad

21.1. El responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

21.2. Para la determinación de las medidas referidas en el numeral anterior, el responsable considerará los siguientes factores:

- a. El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
- b. El estado de la técnica.
- c. Los costos de aplicación.
- d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.
- e. El alcance, contexto y las finalidades del tratamiento.
- f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar.
- g. El número de titulares.
- h. Las posibles consecuencias que se derivarían de una vulneración para los titulares.
- i. Las vulneraciones previas ocurridas en el tratamiento de datos personales.

21.3. El responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.

416. Desde luego, no se desconoce que el despliegue de estas medidas de protección sobre la información recopilada se vincula estrechamente con cuestiones técnicas que justifican el que tenga que ser el órgano especializado en la materia quien a través de la emisión de disposiciones administrativas precise estos aspectos. Sin embargo, para este Tribunal Pleno era necesario que en ley se establecieran al menos condiciones generales, niveles mínimos de protección o estándares a partir de los cuales las disposiciones técnicas pudieran desarrollarse.¹²⁰
417. En consecuencia, no resulta suficiente que el artículo 180 Septimus establezca que la información contenida en el PANAUT será considerada confidencial y reservada, así como tampoco el sistema de sanciones económica previstas por los artículos 307 Bis y 307 Ter, pues como se indicó, la protección efectiva de la privacidad y datos personales de los usuarios, exigía un nivel particularmente elevado de protección y de seguridad mediante medidas técnicas y de gestión adecuadas.
418. No hacerlo así coloca a los derechos humanos a la privacidad y protección de datos personales en una grave situación de riesgo que no puede avalarse.
419. Máxime cuando, además, se advierte que con la emisión del Decreto impugnado se incumplió con el mandato de “*mejores prácticas*” que impone la referida Ley General, pues conforme a su artículo 74, cuando el responsable –lo cual incluye al Congreso de la Unión en términos de los artículos 1 y 3, fracción XXVIII– pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una **evaluación de impacto en la protección de datos personales** y presentarla ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o los Organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.¹²¹
420. En ese sentido, el artículo 75 precisa que se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando: i) existan riesgos inherentes a los datos personales a tratar; ii) se traten datos personales sensibles; y iii) se efectúen o pretendan efectuar transferencias de datos personales.
421. En consecuencia, dado el fuerte impacto que el PANAUT genera en los derechos humanos a la privacidad y protección de los datos personales, y dado que también se afectan los datos sensibles de los usuarios de telefonía móvil, debe concluirse que la emisión del Decreto impugnado requería de una **evaluación de impacto en la protección de datos personales** en términos de la referida Ley General, la cual, de las constancias que integran este expediente, no se advierte que haya existido. No haber cumplido con esta exigencia somete a los derechos a la privacidad, intimidad y protección de datos personales a un riesgo que no puede ser avalado a la luz de los artículos 6 y 16 de la Constitución General.
422. Así, estos incumplimientos por parte del Congreso de la Unión al momento de emitir el Decreto por el cual se crea y regula el PANAUT refuerzan la conclusión alcanzada hasta este punto: una obligación indistinta y generalizada de recabar y conservar información privada e íntima, así como datos personales y sensibles de todos los usuarios de telefonía móvil infringe desproporcionadamente los derechos fundamentales a la privacidad, intimidad y protección de datos personales y resulta incompatible con las exigencias y estándares que impone una sociedad democrática.
423. En consecuencia, lo procedente es declarar la **invalidez del sistema normativo creado por el Decreto de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno.**
424. Sobre este punto, debe reiterarse que el estudio sobre la razonabilidad de la afectación a los derechos humanos en juego abarca **la totalidad de los cambios normativos introducidos por el Decreto impugnado**, puesto que constituye una unidad que no puede disociarse. En efecto, la causa que genera la afectación a los derechos humanos a la privacidad, intimidad y protección de datos personales es **el sistema normativo que crea y regula el PANAUT**, por tanto, si dicha afectación no resulta razonable, la consecuencia es que debe anularse todo el sistema normativo que la genera.

¹²⁰ Al respecto véase al Tribunal de Justicia de la Unión Europea en los casos Digital Rights Ireland Ltd v. Minister for Communications and others, Asunto C-293/12 y C-594/12, sentencia de ocho de abril de dos mil catorce, párr. 54 y 55, 60 a 62 y 66 a 68 y Tele2 Sverige AB y otros, C 203/15 y C-698/15, sentencia de veintiuno de diciembre de dos mil dieciséis, párr. 122 a 124.

¹²¹ Para efectos de claridad en la votación emitida por el Pleno de la Suprema Corte de Justicia de la Nación en las sesiones de los días veinticinco y veintiséis de abril de dos mil veintidós, específicamente, en relación con el voto emitido por el señor Ministro Gutiérrez Ortiz Mena, quien manifestó apartarse de los párrafos 398 a 400 del proyecto de sentencia sometido a consideración del tribunal Pleno, se informa que, derivado de las modificaciones aceptadas en dichas sesiones, tales párrafos pasaron a ser los números 419, 420 y 421 en el presente engrose.

425. Esto queda en evidencia porque, si se invalidan únicamente aquellos preceptos que obligan a los usuarios de telefonía móvil a entregar su información privada, así como sus datos personales y sensibles, el resto del sistema normativo ya no se entiende, pierde su razón de ser.
426. Es por esta razón que este Tribunal Pleno llega a la convicción de que debe anularse **la totalidad del Decreto impugnado, específicamente, todos los artículos que adicionó a la Ley Federal de Telecomunicaciones y Radiodifusión, a saber: la fracción XLII bis del artículo 15, y los artículos 180 Bis, 180 Ter, 180 Quáter, 180 Quintes, 180 Sextus, 180 Septimus, 307 Bis, 307 Ter, 307 Quáter y 307 Quintus, así como los transitorios primero, segundo, tercero, cuarto, quinto y sexto; y por lo que hace a las reformas introducidas a los artículos 176 y 190, fracciones VI y VII de ese ordenamiento, deben invalidarse las porciones normativas reformadas que se precisan en el apartado de efectos.** En esa tesitura, resulta innecesario el estudio de los restantes argumentos formulados por los accionantes.
427. **OCTAVO. Efectos.** De conformidad con el artículo 73, en relación con los numerales 41, 43, 44 y 45, todos de la Ley Reglamentaria de la materia, las sentencias deberán contener los alcances y efectos de la misma, fijando con precisión los órganos obligados a cumplirla, las normas generales respecto de los cuales opere y todos aquellos elementos necesarios para su plena eficacia en el ámbito que corresponda.
428. Como quedó precisado, en el caso la invalidez decretada abarca **la totalidad del sistema normativo** que integra el Decreto de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno, por lo que dicha invalidez surtirá sus efectos a partir de la notificación de los puntos resolutivos de la presente sentencia al Congreso de la Unión.
429. Sin embargo, dado que los artículos 176 y 190, fracciones VI y VII, de la referida legislación fueron los únicos que se reformaron –ya que el resto de los preceptos fueron adiciones–, deben precisarse los efectos que respecto a dichos artículos en concreto tendrá la invalidez decretada a fin de dotar a los operadores jurídicos de certeza sobre las consecuencias de esta resolución.
430. En esa tesitura, tomando en cuenta: *i)* que en ellos se prevén facultades del Instituto Federal de Telecomunicaciones que no tienen que ver con la creación y regulación del PANAUT; *ii)* que en la presente resolución se declara la invalidez del sistema normativo introducido por el **Decreto impugnado**; y *iii)* a fin no generar un vacío normativo que afecte las competencias del Instituto Federal de Telecomunicaciones, este Tribunal Pleno precisa que, en cuanto a dichas normas, la invalidez decretada únicamente tendrá por efecto expulsar del ordenamiento jurídico la porción normativa referida al Padrón Nacional de Usuarios de Telefonía Móvil; de suerte que, a partir de la presente resolución, dichas normas deberán leerse de la siguiente manera:

“Artículo 176. El Instituto llevará el Registro Público de Telecomunicaciones, el cual estará integrado por el Registro Público de Concesiones, ~~el Padrón Nacional de Usuarios de Telefonía Móvil~~ y el Sistema Nacional de Información de Infraestructura, de conformidad con lo dispuesto en la presente Ley y las disposiciones aplicables que se emitan.”

“Artículo 190. ...

I. a V. ...

VI. Realizar la suspensión del servicio de los equipos o dispositivos terminales móviles reportados como robados o extraviados, a solicitud del titular, ~~y realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil.~~

(...)

VII. Realizar el bloqueo inmediato de líneas de comunicación móvil que funcionen bajo cualquier esquema de contratación reportadas por los titulares o propietarios, utilizando cualquier medio, como robadas o extraviadas, ~~y proceder a realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil~~; así como, realizar la suspensión inmediata del servicio de telefonía móvil cuando así lo instruya ~~el Instituto para efectos del Padrón Nacional de Usuarios de Telefonía Móvil~~ o la autoridad competente para hacer cesar la comisión de delitos, de conformidad con lo establecido en las disposiciones administrativas y legales aplicables;

VIII. a XII. ...”

431. Por lo expuesto y fundado, se

RESUELVE:

PRIMERO. Es procedente y fundada la acción de inconstitucionalidad 82/2021 y su acumulada 86/2021.

SEGUNDO. Se declara la invalidez **de la totalidad del sistema normativo** que integra el Decreto de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno, específicamente, de la fracción XLII bis del artículo 15, y los artículos 180 Bis, 180 Ter, 180 Quáter, 180 Quintes, 180 Sextus, 180 Septimus, 307 Bis, 307 Ter, 307 Quáter, y 307 Quintus, así como los transitorios primero, segundo, tercero, cuarto, quinto y sexto, adicionados a la Ley Federal de Telecomunicaciones y Radiodifusión; así como la invalidez de las porciones normativas “, el Padrón Nacional de Usuarios de Telefonía Móvil” del artículo 176, “, y realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil” de la fracción VI del artículo 190, “, y proceder a realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil;” y “el Instituto para efectos del Padrón Nacional de Usuarios de Telefonía Móvil o” de la fracción VII del artículo 190, reformados mediante dicho Decreto.

TERCERO. Las declaratorias de invalidez surtirán sus efectos a partir de la notificación de los puntos resolutivos de esta sentencia al Congreso de la Unión, de conformidad con su considerando octavo.

CUARTO. Publíquese esta resolución en el Diario Oficial de la Federación, así como en el Semanario Judicial de la Federación y su Gaceta.

Notifíquese; haciéndolo por medio de oficio a las partes y, en su oportunidad, archívese el expediente como asunto concluido

Así lo resolvió el Pleno de la Suprema Corte de Justicia de la Nación:

En relación con el punto resolutivo primero:

Se aprobó por unanimidad de once votos de las señoras Ministras y de los señores Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá, Esquivel Mossa, Ortiz Ahlf, Aguilar Morales, Pardo Rebolledo, Piña Hernández, Ríos Farjat, Laynez Potisek, Pérez Dayán y Presidente Zaldívar Lelo de Larrea, respecto de los considerandos primero, segundo, tercero y cuarto relativos, respectivamente, a la competencia, a la precisión de normas impugnadas, a la oportunidad y a la legitimación.

Se aprobó por unanimidad de once votos de las señoras Ministras y de los señores Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá apartándose del párrafo cuarenta y dos del proyecto original, Esquivel Mossa, Ortiz Ahlf, Aguilar Morales, Pardo Rebolledo, Piña Hernández, Ríos Farjat, Laynez Potisek, Pérez Dayán y Presidente Zaldívar Lelo de Larrea en contra de algunas consideraciones, respecto del considerando quinto, relativo a las causas de improcedencia.

En relación con el punto resolutivo segundo:

Se aprobó por unanimidad de once votos de las señoras Ministras y de los señores Ministros Gutiérrez Ortiz Mena apartándose de los párrafos ochenta y tres y ochenta y cinco del proyecto original, González Alcántara Carrancá apartándose de algunas consideraciones, Esquivel Mossa, Ortiz Ahlf, Aguilar Morales apartándose del párrafo ochenta y cinco del proyecto original, Pardo Rebolledo, Piña Hernández, Ríos Farjat, Laynez Potisek, Pérez Dayán y Presidente Zaldívar Lelo de Larrea, respecto del considerando sexto, relativo a las violaciones al proceso legislativo, consistente en reconocer la validez del procedimiento que culminó en el DECRETO por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno. Los señores Ministros Gutiérrez Ortiz Mena y Aguilar Morales anunciaron sendos votos concurrentes.

Se aprobó por mayoría de nueve votos de las señoras Ministras y de los señores Ministros Gutiérrez Ortiz Mena apartándose de algunas consideraciones, González Alcántara Carrancá, Esquivel Mossa, Ortiz Ahlf apartándose de algunas consideraciones, Aguilar Morales por razones adicionales, Pardo Rebolledo, Piña Hernández, Laynez Potisek y Presidente Zaldívar Lelo de Larrea, respecto del considerando séptimo, relativo a la vulneración a los derechos de privacidad, intimidad y protección de

datos personales, consistente en declarar la invalidez del DECRETO por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno, específicamente sus artículos 15, fracción XLII Bis, 176 en su porción normativa “el Padrón Nacional de Usuarios de Telefonía Móvil”, 180 Bis, 180 Ter, 180 Quáter, 180 Quintes, 180 Sextus, 180 Septimus, 190, fracciones VI, en su porción normativa “y realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil”, y VII, en sus porciones normativas “y proceder a realizar el aviso correspondiente en el Padrón Nacional de Usuarios de Telefonía Móvil” y “el Instituto para efectos del Padrón Nacional de Usuarios de Telefonía Móvil o”, 307 Bis, 307 Ter, 307 Quáter y 307 Quintus, así como la de sus artículos transitorios del primero al sexto. La señora Ministra Ríos Farjat votó por la invalidez de los artículos 180 Ter, fracción VI, 180 Quáter, en su porción normativa “comprobante de domicilio y datos biométricos”, 180 Quintes, párrafo primero, en su porción normativa “datos biométricos”, 180 Septimus, párrafo tercero, y transitorios tercero, párrafo segundo, y cuarto del decreto reclamado, así como por la validez del resto de dicho decreto con una interpretación conforme. El señor Ministro Pérez Dayán votó por la invalidez de los artículos 180 Ter, fracciones VI y VII, 180 Quáter en sus porciones normativas “comprobante de domicilio y datos biométricos”, 180 Quintes, párrafo primero, en su porción normativa “datos biométricos y domicilio”, 180 Septimus, párrafo tercero, y transitorios tercero, párrafo segundo, y cuarto del decreto reclamado, así como por la validez del resto de dicho decreto con una interpretación conforme. Las señoras Ministras Esquivel Mossa y Ortiz Ahlf y los señores Ministros Aguilar Morales, Pardo Rebolledo y Laynez Potisek anunciaron sendos votos concurrentes. Los señores Ministros Gutiérrez Ortiz Mena y González Alcántara Carrancá reservaron su derecho de formular sendos votos concurrentes.

En relación con el punto resolutivo tercero:

Se aprobó por unanimidad de diez votos de las señoras Ministras y de los señores Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá, Esquivel Mossa, Ortiz Ahlf, Aguilar Morales, Pardo Rebolledo, Piña Hernández, Ríos Farjat, Laynez Potisek y Presidente Zaldívar Lelo de Larrea, respecto del considerando octavo, relativo a los efectos, consistente en determinar que la declaratoria de invalidez decretada en este fallo surta efectos a partir de la notificación de los puntos resolutivos de esta sentencia al Congreso de la Unión.

En relación con el punto resolutivo cuarto:

Se aprobó por unanimidad de diez votos de las señoras Ministras y de los señores Ministros Gutiérrez Ortiz Mena, González Alcántara Carrancá, Esquivel Mossa, Ortiz Ahlf, Aguilar Morales, Pardo Rebolledo, Piña Hernández, Ríos Farjat, Laynez Potisek y Presidente Zaldívar Lelo de Larrea.

El señor Ministro Alberto Pérez Dayán no asistió a la sesión de veintiséis de abril de dos mil veintidós, previo aviso a la Presidencia.

El señor Ministro Presidente Zaldívar Lelo de Larrea declaró que el asunto se resolvió en los términos precisados. Doy fe.

Firman el señor Ministro Presidente y la señora Ministra Ponente con el Secretario General de Acuerdos, quien da fe.

Ministro Presidente, **Arturo Zaldívar Lelo de Larrea**.- Firmado electrónicamente.- Ministra Ponente, **Norma Lucía Piña Hernández**.- Firmado electrónicamente.- Secretario General de Acuerdos, **Rafael Coello Cetina**.- Firmado electrónicamente.

EL LICENCIADO **RAFAEL COELLO CETINA**, SECRETARIO GENERAL DE ACUERDOS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN: CERTIFICA: Que la presente copia fotostática constante de ochenta y nueve fojas útiles, en las que se cuenta esta certificación, concuerda fiel y exactamente con el original firmado electrónicamente de la sentencia emitida en 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 y diversos Senadores Integrantes de la LXIV Legislatura, dictada por el Pleno de la Suprema Corte de Justicia de la Nación en su sesión del veintiséis de abril de dos mil veintidós. Se certifica con la finalidad de que se publique en el Diario Oficial de la Federación.- Ciudad de México, a siete de noviembre de dos mil veintidós.- Rúbrica.

VOTO CONCURRENTES QUE FORMULA LA MINISTRA LORETTA ORTIZ AHLF, EN LA ACCIÓN DE INCONSTITUCIONALIDAD 82/2021 Y SU ACUMULADA 86/2021.

En las sesiones de veinticinco y veintiséis de abril de dos mil veintidós, el Pleno de la Suprema Corte de Justicia de la Nación analizó y resolvió el asunto citado al rubro y su acumulada, promovidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y diversos Senadores integrantes de la LXIV Legislatura, quienes impugnaron la totalidad de las normas que integran el Decreto de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno, por el que se crea y regula el Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT).

El estudio de fondo en la sentencia se divide en dos apartados principales. El primero, reflejado en el **considerando sexto**, estudia los conceptos de invalidez que hace valer la parte accionante sobre las presuntas violaciones al proceso legislativo.

Al respecto, coincido en con el sentido de la sentencia, así como con las consideraciones que llevan a la conclusión de que: (i) el acto legislativo se encuentra debidamente fundado y motivado; y, (ii) no hubo violaciones al procedimiento legislativo, a pesar de que la votación de las Comisiones se realizó en fechas diferentes.

En el segundo apartado, reflejado en el **considerando séptimo**, la sentencia estudia, propiamente, los conceptos de invalidez encaminados a acreditar la vulneración a los derechos fundamentales a la privacidad, intimidad y protección de datos personales, derivados del Decreto impugnado.

Es aquí en donde si bien coincido con la declaratoria de inconstitucionalidad de las normas impugnadas, me separo de algunas consideraciones, y llego a dicha conclusión por otras distintas.

Con el fin de expresar mi disenso, dividiré dichas consideraciones en las siguientes cuestiones: (i) la importancia de salvaguardar los derechos humanos a la privacidad, intimidad y protección de datos personales, en temas relacionados con la seguridad pública; (ii) la metodología de análisis del decreto impugnado a partir de un sistema normativo; (iii) el uso del test de escrutinio estricto para el análisis de medidas que involucren el derecho a la intimidad; y, (iv) el análisis de la grada de necesidad, como parte del test de escrutinio ordinario.

I. Derechos humanos a la privacidad, intimidad y protección de datos personales y su con la seguridad pública.

La protección a los datos personales reconocida en el artículo 16 constitucional y en el *corpus iuris* internacional en la materia, ha adquirido una gran relevancia, ya que la información de una persona en su ámbito personal y privado se ha vuelto un eje central en la transformación de nuestra sociedad en una “sociedad de la información”.

La generación de datos por parte de un individuo y el tráfico de éstos se ha multiplicado, sin que ello implique que se haya dejado de lado el derecho a la privacidad, por el contrario, la protección de los datos personales es una expresión de este derecho, pues salvaguarda precisamente información que se refiere a la vida privada de las personas y que tiene un gran impacto en otros derechos.

Por esto, en una sociedad como la nuestra, es claro que existe la necesidad imperiosa de que el Estado busque, por un lado, salvaguardar la seguridad nacional y la seguridad pública; y al mismo tiempo, garantizar los derechos humanos a la privacidad, intimidad y protección de datos personales de todas las personas, los cuales son presupuesto para el goce y disfrute de otros derechos humanos.

La seguridad pública y la seguridad ciudadana se enmarcan en un concepto relativamente novedoso que la Corte Interamericana de Derechos Humanos (Corte IDH) denomina como “seguridad ciudadana”.¹

Dicho concepto se ha consolidado en el ámbito internacional, a partir de la noción de “seguridad humana”, que fue acuñado en el ámbito de la Organización de las Naciones Unidas. Retomado de dicho ámbito, la Corte IDH entiende la seguridad ciudadana como “una modalidad específica de la seguridad humana, que puede ser definida inicialmente como la protección universal contra el delito violento o predatorio”.² En concreto, podemos entenderla como “la protección de ciertas opciones u oportunidades de todas las personas –su vida, su integridad, su patrimonio– contra un tipo específico de riesgo (el delito) que altera en forma súbita y dolorosa la vida cotidiana de las víctimas”.³

¹ Corte IDH. Caso Alvarado Espinoza y otros Vs. México. Fondo, Reparaciones y Costas. Sentencia de 28 de noviembre de 2018. Serie C No. 370, nota al pie. 391.

² *Ídem*

³ *Ídem*

Es así que la protección de la seguridad ciudadana es una obligación de los Estados que implica garantizar la seguridad y mantener el orden público, así como perseguir los delitos cometidos en su jurisdicción.⁴

De manera particular, sobre las actividades que son realizadas por el crimen organizado, la Corte IDH ha reconocido que tienen una naturaleza y complejidad tal, que resultan una grave amenaza contra la comunidad internacional, al vulnerar no solo la seguridad, sino también la estabilidad y gobernabilidad democrática de los Estados, a partir de lo cual dificulta su desarrollo e imposibilita que se garanticen los derechos humanos de las personas sujetas a su jurisdicción.⁵

Es así que los Estados tienen la obligación constitucional⁶ y convencional⁷ de tomar todas las acciones necesarias para combatir el crimen organizado y con ello garantizar la seguridad ciudadana de sus gobernados. No obstante, dicha obligación se encuentra limitada al respeto de los demás derechos humanos que conforman el parámetro de control constitucional, compuesto por los derechos humanos que gozan todas las personas.⁸ En otras palabras, los Estados no pueden alegar situaciones excepcionales como medio para suprimir, denegar, desnaturalizar o privar a las personas de sus derechos humanos.⁹

Es ahí, donde cobran relevancia los derechos a la privacidad, intimidad y protección de datos personales de todas las personas, como límite a las acciones que tomen los Estados para cumplir con su obligación.

El sistema normativo impugnado en la presente acción de inconstitucionalidad, que crea al PANAUT, se relaciona con dos derechos en particular: (i) el derecho a la privacidad; y, (ii) el derecho a la intimidad.

El derecho a la privacidad protege el derecho a una “esfera de privacidad” del individuo en contra de las incursiones externas que limitan la capacidad para tomar ciertas decisiones a través de las cuales se ejerce la autonomía personal.¹⁰ Dicha esfera puede ser vulnerada a partir de cierto uso que se pueda dar a los datos personales, tales como el nombre o número de teléfono.

El derecho a la intimidad, por su parte, si bien forma parte del derecho a la privacidad, se ha entendido que cuenta con mayor protección porque se concibe como esencial para la vida privada, que se encuentra a lo reservado y la intimidad. La intimidad, es susceptible a ser vulnerada con el uso de datos sensibles como el domicilio de una persona, sus datos biométricos o la Clave Única de Registro de Población.

El sistema normativo impugnado que crea el PANAUT, impone la obligación de los usuarios de telefonía móvil de entregar algunos datos al Instituto Federal de Telecomunicaciones, para constituir a dicho padrón como “una herramienta que sea útil y permita colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos, específicamente a través de la identificación de los usuarios de una determinada línea telefónica móvil”.¹¹

Para ello, el artículo 180 Ter impugnado, establece en diez fracciones, la información que deberá contener el padrón nacional y que, por tanto, estaría al alcance de las autoridades de seguridad de procuración y administración de justicia, que conforme a las atribuciones previstas en sus leyes aplicables cuenten con la facultad expresa para requerir al Instituto los datos del PANAUT.¹²

La sentencia reconoce que la información requerida a las personas en el sistema normativo impugnado no es homogénea. Alguna de ella, como los datos biométricos de las personas, se puede catalogar como datos sensibles, que pudieran tener un impacto en el derecho a la intimidad; mientras que otra, es susceptible de afectar el derecho a la privacidad.

⁴ Corte IDH. Caso Alvarado Espinoza y otros Vs. México. Fondo, Reparaciones y Costas. Sentencia de 28 de noviembre de 2018. Serie C No. 370, párr. 177; Caso Velásquez Rodríguez Vs. Honduras, Fondo, supra, párr. 154, y Caso del Penal Miguel Castro Castro Vs. Perú. Fondo, Reparaciones y Costas. Sentencia de 25 de noviembre de 2006. Serie C No. 160, párr. 240.

⁵ Corte IDH. Caso Alvarado Espinoza y otros Vs. México. Fondo, Reparaciones y Costas. Sentencia de 28 de noviembre de 2018. Serie C No. 370, párr. 178.

⁶ Artículo 1º, en relación con el diverso 21 de la Constitución Política de los Estados Unidos Mexicanos.

⁷ Artículos 1.1 y 2 de la Convención Americana sobre Derechos Humanos.

⁸ Corte IDH. Caso Alvarado Espinoza y otros Vs. México. Fondo, Reparaciones y Costas. Sentencia de 28 de noviembre de 2018. Serie C No. 370, para. 178; Caso Bulacio Vs. Argentina. Fondo, Reparaciones y Costas. Sentencia de 18 de septiembre de 2003. Serie C No. 100, párr. 124, y Caso del Penal Miguel Castro Castro Vs. Perú. Supra, párr. 240.

⁹ Corte IDH. Caso Pollo Rivera y otros Vs. Perú. Fondo, Reparaciones y Costas. Sentencia de 21 de octubre de 2016. Serie C No. 319, párr. 100. La Convención Americana admite la suspensión de garantías individuales en su artículo 27.1, aunque únicamente en caso de guerra, de peligro público o de otra emergencia que amenace la independencia o seguridad del Estado. Sin embargo, la suspensión de garantías no debe exceder la medida de lo estrictamente necesario y resulta ilegal toda actuación de los poderes públicos que desborde aquellos límites que deben estar precisamente señalados en las disposiciones que decretan el estado de excepción.

¹⁰ Corte IDH. Caso Fernández Prieto y Tumbeiro Vs. Argentina. Fondo y Reparaciones. Sentencia de 1 de septiembre de 2020, párr. 102. La Corte IDH ha precisado, respecto al artículo 11 de la Convención Americana, que, si bien esa norma se titula “Protección de la Honra y de la Dignidad”, su contenido incluye, entre otros, la protección de la vida privada. En ese sentido, la Corte ha sostenido que el ámbito de la privacidad personal y familiar protegido por dicho precepto se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública.

¹¹ Artículo 180 bis impugnado.

¹² Artículo 180 septimus impugnado.

Con base en esta distinción, así como con algunas otras consideraciones, es que quisiera señalar algunos inconvenientes con la metodología adoptada en la sentencia, haciendo un análisis de constitucionalidad sobre un “sistema normativo”.

II. Metodología de análisis de constitucionalidad de un sistema normativo.

En el caso concreto, no comparto la metodología utilizada en la sentencia. Como se puede observar de la línea jurisprudencial de este Alto Tribunal, la metodología de análisis de normas que se aducen inconstitucionales varía caso por caso. Cada una de las personas Ministras que conformamos este Alto Tribunal, hemos optado por la metodología de análisis que más consideramos adecuada al caso concreto, sin que exista un criterio o parámetro establecido o acordado, para determinar cuándo se debe optar una metodología concreta.

En el caso concreto la sentencia plantea que el decreto impugnado en su totalidad debe analizarse como un “sistema normativo”, ya que:

“[...] de la **lectura integral de los conceptos de invalidez** se aprecia que los argumentos a partir de los cuales se plantea la vulneración a los derechos a la privacidad, intimidad y protección de datos personales, abarcan la totalidad de las normas que integran el referido Decreto en tanto se impugnan como sistema normativo”.¹³

“102. En efecto **la afectación alegada a los derechos humanos en juego se hace derivar directamente de la creación y regulación del PANAUT**, dado que se estima que la creación de esta base de datos y la forma en la que se encuentra regulado genera una intromisión injustificada y desproporcionada en tales prerrogativas fundamentales. En esa tesitura, la respuesta que debe brindarse sobre si dicha intromisión es o no justificada, abarca necesariamente el sistema normativo que da lugar a dicha base de datos”.¹⁴ (énfasis añadido)

Si bien coincido en que todas las normas del decreto deben declararse inválidas, destaco a continuación dos razones principales por las que considero que el análisis de la reforma impugnada como un “sistema normativo” podría no haber sido el más conveniente en el estudio del caso concreto.

Primera razón.

Como ya lo adelantaba, el hecho de que la misma sentencia reconozca que el decreto contenga datos que ameriten un análisis diferenciado -datos sensibles, por un lado, y datos personales, por el otro-, para mí es razón suficiente para que en el estudio del decreto impugnado se hubiera adoptado una metodología distinta.

La necesidad de este análisis diferenciado, lo propone la misma sentencia, en el segundo punto del apartado A, del considerando séptimo, titulado “Segunda etapa. Análisis de las distintas gradas que integran la prueba de proporcionalidad”. Aquí se establece que: (i) las injerencias al derecho a la privacidad y la protección de los datos personales en general deben ser analizadas por el *test de escrutinio ordinario*; y, (ii) por lo que hace al derecho a la intimidad y a la protección de los datos sensibles, debe ser analizado a la luz de un *escrutinio estricto*.

En ese sentido, la sentencia concluye que todo el sistema normativo se analizará primero, a la luz del test de proporcionalidad en sentido ordinario, y posteriormente, ese mismo sistema será analizado a la luz de dicho test en su vertiente estricta.

Con independencia de que no coincido con el uso del *test de escrutinio estricto*, para determinar la razonabilidad de la medida con relación a las restricciones al derecho a la intimidad y a la protección de los datos sensibles -lo cual abordaré con mayor profundidad en el siguiente apartado- me parece que resulta contradictorio analizar un mismo sistema normativo a la luz de dos escrutinios distintos.

Un mismo sistema normativo no debería analizarse, primero, a la luz del *escrutinio ordinario*, para que, en el caso de que se supere, de nueva cuenta, todo el sistema normativo en su conjunto deba analizarse bajo un *escrutinio estricto*.

Si bien, en el caso concreto, no hubo necesidad de caer en dicha contradicción, ya que la medida no superó la tercera grada del *test de proporcionalidad ordinario*; en el supuesto de que sí lo hubiera superado, considero que hubiéramos caído en una grave contradicción metodológica, a partir de las siguientes consideraciones:

¹³ Párrafo 101 de la sentencia de la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021.

¹⁴ Párrafo 102 de la sentencia de la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021.

- a) La aplicación del *test de escrutinio ordinario*, parte de la premisa de que la norma impugnada es constitucional. Por el contrario, al analizar una norma bajo el *escrutinio estricto*, se parte de la premisa de que ésta es inconstitucional.

De esta forma, considero equívoco que, al mismo tiempo, tengamos que partir de la premisa de que una medida es constitucional e inconstitucional.

- b) Para el análisis de la primera grada del *test de escrutinio ordinario*, se debe analizar si la medida busca una finalidad constitucionalmente **válida**. Para su vertiente *estricta*, la primera grada lo que analiza, es si ésta persigue un fin constitucionalmente **imperioso**.

Como ya ha sido estudiado por este Máximo Tribunal, mientras que el análisis de una finalidad constitucional imperativa implica que su consecución sea a través de los medios menos gravosos posibles, exigiendo una máxima racionalidad al legislador; en el *escrutinio ordinario* sólo se exige la legitimidad de una finalidad admisible y una relación racional entre ésta y la medida exigiendo una mínima racionalidad.¹⁵

Segunda razón.

Considero que si bien, en ocasiones puede ser pertinente, e incluso necesario, hacer el análisis de constitucionalidad de un sistema normativo en su conjunto; lo cierto es que dependiendo del caso concreto pudiera existir un riesgo fundado, de que este Máximo Tribunal analizara la idoneidad o eficacia de una política pública, más allá de los vicios de constitucionalidad que podrían tener algunos de sus elementos.

Bajo mi consideración, por regla general, el estudio de un decreto impugnado debería partir de un análisis individualizado de las normas o porciones normativas que sean impugnadas, a pesar de que los argumentos de las o la parte accionante, no se hayan focalizado de manera independiente y particularizada.

Lo anterior, me parece que garantiza el principio de división de poderes, sin que de manera indirecta este Tribunal Pleno se pronunciara sobre la idoneidad de una política pública, en este caso criminal, más allá de su constitucionalidad. Ello, sin que eso signifique que la Suprema Corte de Justicia de la Nación deje de desempeñar su papel de máximo intérprete de la Constitución y protector de los intereses más sensibles de las personas y comunidades de nuestra sociedad ya que, sin duda alguna, su actuar ha tenido una vocación transformadora.

Si bien sostengo que como regla general, para mí el análisis de un decreto impugnado, amerita un estudio individualizado de las normas que lo integran, lo cierto es que excepcionalmente la metodología de análisis, sí podría hacerse de manera holística, como un sistema normativo en su conjunto, siempre que: (i) las normas impugnadas no puedan subsistir de manera evidente, a partir de la invalidación de otras, por lo que las mismas se tornen inoperantes; o (ii) si a pesar de lo anterior, la invalidación de ciertas porciones sean la razón de ser que motiva la reforma impugnada.

Bajo esta lógica, la razón por la cual considero que, en este caso, es plausible analizar el decreto impugnado a partir de un “sistema normativo”, es por las excepciones que referí en el párrafo anterior. En otras palabras, se podría considerar viable que, al invalidar ciertas porciones normativas, se podría desarticular todo el sistema normativo, o en su caso, perdería su razón de ser, a la luz de la finalidad constitucionalmente válida del decreto.

III. Elección del escrutinio del test de proporcionalidad para el análisis de la reforma impugnada.

No coincido en que el caso concreto deba analizarse a partir de un test de *escrutinio estricto*. Como adelanté, la sentencia concluye que el decreto impone restricciones relacionadas con datos personales que vulneran el derecho a la privacidad, las cuales deben ser analizadas desde un *escrutinio ordinario*, y otras relacionadas con datos o información sensible que podría vulnerar el derecho a la intimidad, las cuales deben ser observadas bajo un *escrutinio estricto*.

De manera concreta, el párrafo 214 de la sentencia establece que “el test de *escrutinio estricto* es exigible en dos supuestos generales: i) cuando se combaten distinciones legislativas que se apoyan en una de las denominadas categorías sospechosas previstas en el artículo 1 constitucional; o ii) cuando la norma opera sobre derechos fundamentales especialmente sensibles que dadas sus condiciones o importancia en determinados supuestos, exigen una tutela reforzada, de tal suerte que con este escrutinio se busca garantizar que la medida analizada tenga una justificación robusta que derrote la presunción de inconstitucionalidad que pesa sobre ella”.

¹⁵ Sentencia recaída al amparo directo en revisión 4292/2019, de la Primera Sala de la SCJN, en su sesión del 24 de marzo de 2021. Ministro Ponente: Alfredo Gutiérrez Ortiz Mena.

A partir de un análisis de los casos resueltos por este Alto Tribunal, en los últimos años, no comparto que el *test de escrutinio estricto* se utilice para analizar datos que afectan la intimidad de las personas, ya que no considero que ello se trate de un análisis de derechos especialmente sensibles que, dadas sus condiciones o importancia en determinados supuestos, exigen una tutela reforzada.

La gran mayoría de las ocasiones en que este Alto Tribunal ha hecho uso del *test de escrutinio estricto* para determinar si una distinción es proporcional, han sido asuntos que analizan medidas que involucran alguna de las denominadas “categorías sospechosas” reconocidas en el artículo 1° constitucional, u otras reconocidas en otros tratados internacionales,¹⁶ siempre que éstas no constituyan medidas afirmativas.

En el resto de los casos en que se ha utilizado dicho test, ha sido para el análisis de medidas que tienen que ver con restricciones a la libertad de expresión de los partidos políticos,¹⁷ e incluso en dichas ocasiones el criterio de los integrantes del Pleno no ha sido unánime al respecto.¹⁸

Sin que mi opinión en este voto, adelante mi criterio para este segundo tipo de asuntos en que se ha aplicado el *escrutinio estricto*; considero que en el caso que nos ocupa, no es necesario el estudio del sistema normativo a partir de un *escrutinio estricto*.

En el caso concreto, no me parece evidente que la creación del PANAUT, a raíz de la entrega de datos sensibles, vulnere de manera expresa la Constitución. La gran diferencia del análisis a partir de un *escrutinio estricto* es que con éste se parte de la premisa de que la norma es inconstitucional, lo cual, *a contrario sensu*, implica que estaríamos haciendo un análisis de inconstitucionalidad, más que de constitucionalidad.

En el caso que nos ocupa, estimo que el mero hecho de que la medida persiga un fin legítimo, e incluso imperioso, como lo es la seguridad pública, derivada de una situación identificada de delitos de gran relevancia que se cometen a partir de dispositivos móviles, da motivos suficientes para que el análisis del sistema normativo parta de la presunción de constitucionalidad de la norma.

Finalmente, en congruencia con lo anterior, me separo del párrafo 215 que establece la necesidad de aplicar ambos escrutinios, lo cual, además, estimo que contrasta con el contenido de los párrafos 393 a 402, en los cuales se concluye que es innecesario desarrollar el *test de escrutinio estricto*.

IV. Análisis de la grada de necesidad, como parte del test de escrutinio ordinario.

El análisis de una medida a partir del *test de escrutinio ordinario* implica el estudio a partir de 4 gradas, para saber si la medida: (i) persigue una **finalidad constitucionalmente válida**; (ii) es **idónea** para la consecución de dicha finalidad; (iii) constituye una medida **necesaria**; y, (iv) es **proporcional** en sentido estricto.

En el caso concreto, coincido con la sentencia en el sentido de que el sistema normativo impugnado supera las dos primeras gradas del *test de escrutinio ordinario*. Ahora, si bien, coincido con la sentencia en que la medida legislativa impugnada no supera la tercera grada de dicho test de proporcionalidad, esto es, la necesidad de la medida, lo cierto es que me separo de algunas consideraciones que retoma la sentencia.

De acuerdo con la línea jurisprudencial de este Alto Tribunal, la razón de ser de la tercera grada del *test de proporcionalidad en su escrutinio ordinario* (necesidad) es conocer si existen otras medidas que resulten igualmente idóneas para lograr los fines que se persiguen, con el fin de corroborar que no existan otras alternativas menos lesivas al derecho que se está limitando, o que intervengan con menor intensidad en el mismo.

Así, de encontrarse alguna medida alternativa que sea igualmente idónea para proteger el fin constitucional y que a su vez intervenga con menor intensidad al derecho, deberá concluirse que la medida elegida por el legislador es inconstitucional. En caso contrario, deberá pasarse a la cuarta y última etapa del escrutinio: la proporcionalidad en sentido estricto.

¹⁶ Convención Americana sobre Derechos Humanos, Pacto Internacional de Derechos Civiles y Políticos, Pacto Internacional de Derechos Económicos, Sociales y Culturales, entre otros.

¹⁷ Acción de inconstitucionalidad 132/2020; acciones de inconstitucionalidad 35/2014 y sus acumuladas 74/2014, 76/2014 y 83/2014; 45/2014 y sus acumuladas 46/2014, 66/2014, 67/2014, 68/2014, 69/2014 y 75/2014; 129/2015 y sus acumuladas 130/2015, 131/2015, 132/2015, 133/2015 y 137/2015; 64/2015 y sus acumuladas 65/2015, 66/2015, 68/2015 y 70/2015; 50/2015 y sus acumuladas 55/2015, 56/2015 y 58/2015; y, 67/2015 y sus acumuladas 72/2015 y 82/2015.

¹⁸ Al respecto, se puede observar la discusión de la acción de inconstitucionalidad 132/2020, del 21 de septiembre de 2020, en donde, de la mayoría de las y los 9 Ministros que votaron por la invalidez de la norma, 4 votaron por que no se debía usar un escrutinio estricto (Ministros Laynez Potisek, Juan Luis González Alcántara Carrancá, Luis María Aguilar Morales y Ana Margarita Ríos Farjat); mientras que 5 votaron por que sí debía analizarse bajo este escrutinio.

Para desarrollar el examen de necesidad, la sentencia estudia otras medidas o mecanismos que considera igualmente idóneos para lograr los fines que persigue el PANAUT, y que resulten menos lesivos para los derechos afectados.

Al respecto, estimo que dos de ellas son analizadas de tal manera que pareciera que este Pleno se está pronunciando sobre su constitucionalidad: (i) la intervención de comunicaciones (párrafos 288 a 354); y, (ii) la geolocalización y entrega de datos (párrafos 355 a 375).

Desde mi punto de vista, el análisis de la tercera grada no tiene que profundizar sobre el estudio de dichas alternativas. Tal como lo resolvió la Primera Sala de este Alto Tribunal, en el amparo en revisión 237/2014, sobre esta grada del test, “la búsqueda de medios alternativos podría ser interminable y requerir al juez constitucional imaginarse y analizar todas las alternativas posibles. No obstante, dicho escrutinio puede acotarse ponderando aquellas medidas que el legislador consideró adecuadas para situaciones similares o bien las alternativas que en el derecho comparado se han diseñado para regular el mismo fenómeno. En cualquier caso, conviene aclarar que la comparación entre regulaciones en el marco del análisis de necesidad de una medida cumple la función de acotar el universo de alternativas que el legislador pudo considerar al momento de afectar el derecho en cuestión”.

En ese sentido, resulta innecesario hacer un análisis profundo de las medidas alternas que sean menos lesivas para la consecución de la finalidad establecida. El riesgo de lo anterior es que la sentencia, de manera indirecta, realice un análisis de constitucionalidad a partir de un test de proporcionalidad de medidas, que efectivamente ya existen en el ordenamiento jurídico mexicano.

Más aún, el hecho de afirmar que dichas medidas superan, por lo menos, las primeras tres gradas del *escrutinio ordinario* del test de proporcionalidad, podría leerse como una limitación para que los demás poderes, no busquen el establecimiento de medidas para luchar por la seguridad pública del país, en clave de que ya existen las medidas legislativas suficientes para ello.

Ahora, a pesar de que no paso por alto el párrafo 287 de la sentencia que establece que “no tiene por objeto revisar la validez constitucional de las diversas figuras, ni compromete en sentido alguno el criterio de este Tribunal Pleno sobre tal aspecto, puesto que lo único que se pretende realizar es un estudio comparativo frente al PANAUT a fin de poder determinar si dichos mecanismos resultan igualmente idóneos, pero son menos restrictivos de los derechos humanos a la privacidad y protección de datos personales”, lo cierto es que las consideraciones de este Pleno que son aprobadas por mayoría de 8 votos resultan obligatorias para todas las autoridades jurisdiccionales de la Federación y las entidades federativas, aun cuando se incluya dicha acotación.

En ese sentido, me aparto de aquellos razonamientos que analizan las medidas relacionadas con la intervención de comunicaciones y geolocalización.

En concordancia con lo anterior, también me aparto de las preguntas que se plantea la sentencia en el párrafo 390 del proyecto, en donde se cuestiona si el decreto impugnado “realmente” era necesario, ya que “existen otras herramientas” para lograr el fin analizado.

Lo anterior ya que, en mi opinión, solo refuerza la idea de que las medidas existentes ya son suficientes para lograr el fin planteado, lo cual, me parece, no es tarea para que este Alto Tribunal determine.

ATENTAMENTE

Ministra **Loretta Ortiz Ahlf**.- Firmado electrónicamente.- Secretario General de Acuerdos, Lic. **Rafael Coello Cetina**.- Firmado electrónicamente.

EL LICENCIADO **RAFAEL COELLO CETINA**, SECRETARIO GENERAL DE ACUERDOS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN: CERTIFICA: Que la presente copia fotostática constante de ocho fojas útiles, concuerda fiel y exactamente con el original firmado electrónicamente del voto concurrente formulado por la señora Ministra Loretta Ortiz Ahlf, en relación con la sentencia del veintiséis de abril de dos mil veintidós, dictada por el Pleno de la Suprema Corte de Justicia de la Nación en 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 y diversos Senadores Integrantes de la LXIV Legislatura. Se certifica con la finalidad de que se publique en el Diario Oficial de la Federación.- Ciudad de México, a siete de noviembre de dos mil veintidós.- Rúbrica.

VOTO CONCURRENTES QUE FORMULA EL MINISTRO JUAN LUIS GONZÁLEZ ALCÁNTARA CARRANCÁ EN LA ACCIÓN DE INCONSTITUCIONALIDAD 82/2021 Y SU ACUMULADA 86/2021.

1. En la sesión celebrada el veintiséis de abril de dos mil veintidós, el Pleno de la Suprema Corte de Justicia de la Nación resolvió como procedente y fundada 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 integrantes de la LXIV Legislatura. En éstas, se declaró la invalidez de la totalidad del sistema normativo que integra el decreto de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión (en adelante “LFTR”), publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno, y por el cual se creó y reguló el Padrón Nacional de Usuarios de Telefonía Móvil (en adelante “PANAUT”).
2. Cabe señalar que el PANAUT era una base de datos integrada por información personal e íntima de los titulares de cada línea de telefonía móvil, incluyendo nombre completo, nacionalidad, número de identificación oficial con fotografía, Clave Única de Registro de Población, datos biométricos y domicilio, entre otros. Su instalación, operación, regulación y mantenimiento estaba a cargo del Instituto Federal de Telecomunicaciones. La finalidad de la base de datos, de acuerdo con el artículo 180 bis de la LFTR, era contar con una herramienta útil que permitiera colaborar con las autoridades del Estado en materia de seguridad y justicia en asuntos relacionados con la comisión de ciertos delitos, específicamente, a través de la identificación de los usuarios de una determinada línea telefónica móvil. Para ello, las normas preveían como obligatorio para los usuarios el registro de su línea de teléfono celular ante los concesionarios de telecomunicaciones.
3. Tal como señalé en mi intervención, me parece que la creación de dicho padrón partía de una premisa equivocada y peligrosa: la dicotomía entre seguridad y privacidad. Ésta exige a los ciudadanos entregar datos personales y ceder su privacidad frente al Estado a cambio de mayor seguridad. Con más información de los ciudadanos, el Estado tiene mayor control sobre ellos y puede protegerlos. Esta lógica no solamente contraría los valores democráticos que el Estado Mexicano reconoce en su Constitución, sino que ignora que: 1) más información no garantiza más seguridad; y, 2) la creación de bases de datos centralizadas como éstas acarrearán un riesgo para los ciudadanos. En México, contamos con un claro ejemplo de esto: el fallido Registro Nacional de Usuarios de Telefonía Móvil (conocido como RENAUT), creado en 2009. Tal como se desarrolla más abajo, el RENAUT fue ineficaz en mejorar la seguridad de los usuarios. Además, contrario a lo esperado, el RENAUT puso en mayor riesgo a los usuarios de telefonía móvil al filtrarse y, por eso, se tomó la decisión de destruirlo en 2011. Sin embargo, esta base de datos ya se encontraba en el mercado ilegal.¹
4. En el estudio de fondo, el Tribunal Pleno concluyó que el PANAUT vulneraba los derechos de privacidad, intimidad y protección de datos personales, y la mayoría acordamos que debía invalidarse la totalidad del sistema normativo del PANAUT. En general, me expresé de acuerdo con los argumentos presentados por la Ministra ponente en el asunto. Sin embargo, me separé de algunas consideraciones específicas del proyecto estudiado por las razones que expreso en este voto concurrente. La primera, versa sobre las causales de improcedencia (I); la segunda, relativa a la metodología del estudio de fondo (II); y la tercera, respecto al test de proporcionalidad realizado (III).

I. Divergencia en las causales de improcedencia.

5. Durante la discusión de las causales de improcedencia, me separé del párrafo 42 del proyecto (que en el engrose equivale al párrafo 43).² Dicho párrafo responde a un argumento del informe del Poder Ejecutivo Federal, por el cual alegaba que el INAI carecía de legitimación para hacer valer violaciones al proceso legislativo, así como para plantear la vulneración a los principios de interés superior del menor, no retroactividad de la ley en perjuicio de las personas y presunción de inocencia.

¹ Véase “Ofertan RENAUT en la red en 500 pesos” Solís, Víctor. *El Universal*. 3 de junio de 2010. <<https://archivo.eluniversal.com.mx/nacion/178140.html>>

² El párrafo referido señala lo siguiente:

“No obstante, este Tribunal Pleno estima que no asiste la razón al Ejecutivo Federal pues la legitimación del Instituto promovente, de conformidad con el artículo 105, fracción II, inciso h), constitucional debe evaluarse en función del acto que se impugna y su vinculación con la afectación a los derechos humanos de acceso a la información y protección de datos personales, **no en función de los argumentos que se hacen valer para proteger tales derechos.**”

6. En el párrafo 42 (ahora 43), la mayoría estimó que no asistía la razón al Ejecutivo Federal porque la legitimación del Instituto promovente, de conformidad con el artículo 105, fracción II, inciso h), constitucional³ debe evaluarse en función del acto que se impugna y su vinculación con la afectación de los derechos humanos de acceso a la información y protección de datos personales, no en función de los argumentos que se hacen valer para proteger tales derechos. Me parece que con tal afirmación lo que se pretende decir es que, en este caso, las violaciones a los principios de interés superior del menor, no retroactividad de la ley en perjuicio de las personas y presunción de inocencia deben entenderse como argumentos en función de la protección de los derechos de acceso a la información y protección de datos personales. Más aún, lo importante es que las normas impugnadas que creaban el PANAUT estaban directa y evidentemente vinculadas a la afectación al derecho de protección de datos personales porque implicaban la recolección y el tratamiento de datos personales.
7. No obstante de que estoy de acuerdo en que no asistía la razón al Ejecutivo Federal en su dicho, pues en este caso es evidente que el acto impugnado estaba vinculado al derecho de protección de datos personales, me separé de la afirmación del referido párrafo porque me parece que su redacción nos lleva a conclusiones equivocadas. En particular, creo que es equivocado decir que únicamente debe evaluarse la legitimación del INAI en función del acto que se impugna y la vinculación de éste con los derechos de acceso a la información y protección de datos personales. Si bien, en este caso tal vinculación es directa y evidente, no siempre es así, y la argumentación es entonces necesaria para demostrar la afectación a los derechos. No considerar los argumentos podría llevar a concluir equivocadamente que una demanda es improcedente por no existir relación con dichos derechos. Así pues, contrario a lo que señala el párrafo del que me separé, considero que para determinar la legitimación del Instituto promovente es importante considerar tanto el acto impugnado como los argumentos que se hacen valer, que podrían evidenciar una vulneración indirecta o menos obvia a los derechos de acceso a la información y protección de datos personales.

II. Divergencias en cuanto a la metodología.

A. Consideraciones de la mayoría.

8. La resolución analiza la totalidad de los preceptos que integran el decreto y que conformaban el sistema normativo que creaba y regulaba el PANAUT, y utiliza como eje toral el núcleo de la impugnación de los accionantes: la vulneración de los derechos humanos a la privacidad, intimidad y protección de datos personales. Como metodología, opta por realizar una prueba de proporcionalidad.
9. Tras identificar que la regulación del PANAUT tiene un impacto *prima facie* en los derechos de privacidad, intimidad y protección de datos personales, y subrayar que dicha intromisión es intensa, el estudio considera necesario elegir el nivel de escrutinio que deberá realizarse. Opta por segmentar el análisis: considera que las intromisiones a la intimidad y la protección de datos sensibles deben ser analizadas a la luz de un escrutinio estricto, dado que el derecho a la intimidad requiere de una especial protección. Mientras que las injerencias al derecho a la privacidad y la protección de los datos personales deben ser revisadas a la luz de un escrutinio ordinario.

B. Razones de la concurrencia.

10. Me parece adecuada la utilización de un test de proporcionalidad porque, en efecto, nos enfrentamos ante un caso en el que los derechos a la privacidad, la intimidad y la protección de datos personales se deben ponderar frente al objetivo que plantea la norma de combatir a la delincuencia.

³ "Artículo 105. La Suprema Corte de Justicia de la Nación conocerá, en los términos que señale la ley reglamentaria, de los asuntos siguientes:

[...]

II. De las acciones de inconstitucionalidad que tengan por objeto plantear la posible contradicción entre una norma de carácter general y esta Constitución.

Las acciones de inconstitucionalidad podrán ejercitarse, dentro de los treinta días naturales siguientes a la fecha de publicación de la norma, por:

[...]

h) El organismo garante que establece el artículo 6° de esta Constitución en contra de leyes de carácter federal y local, así como de tratados internacionales celebrados por el Ejecutivo Federal y aprobados por el Senado de la República, que vulneren el derecho al acceso a la información pública y la protección de datos personales. Asimismo, los organismos garantes equivalentes en las entidades federativas, en contra de leyes expedidas por las Legislaturas locales; e"

11. Es cierto que, tal como lo señala la Constitución Federal, la protección de datos personales puede restringirse por razones de seguridad pública y para la protección de derechos de terceros.⁴ Sin embargo, la restricción al derecho debe ser proporcional. Así pues, realizar un test de proporcionalidad para estudiar la medida es adecuado y pertinente.
12. Cabe señalar que el principio de proporcionalidad es un principio del tratamiento de datos personales, reconocido por las Leyes en la materia de México,⁵ y por el artículo 5, inciso C, del Convenio N° 108 del Consejo de Europa en materia de datos personales, del cual México forma parte.⁶ Por ello, la realización de una prueba de proporcionalidad es particularmente adecuada para examinar este derecho.
13. Sin embargo, difiero de la mayoría en cuanto a que considero que no es necesario segregar el test en distintos niveles de escrutinio. Considero, tal como lo he expresado con anterioridad, que los niveles de escrutinio —estricto y ordinario— son pertinentes para la realización del examen de igualdad, pero no para el de proporcionalidad. Si bien, estoy de acuerdo en que nos encontramos frente a afectaciones a derechos especialmente sensibles que exigen una tutela reforzada, considero que los pasos del test de proporcionalidad permiten valorar en mayor o menor grado los derechos protegidos frente a la medida estudiada, sin que resulte necesario de antemano elevar su nivel de escrutinio.

III. Divergencia en cuanto al análisis del test de proporcionalidad.

A. Consideraciones de la mayoría.

14. Tras señalar que se debe segmentar el análisis por niveles de escrutinio, el estudio inicia el análisis realizando el test en escrutinio ordinario. La primera grada del test se supera porque el acto impugnado contaba con un fin constitucionalmente válido. La medida legislativa perseguía fines de interés público relacionados con el fortalecimiento de las herramientas para la investigación y persecución de los delitos. Estas finalidades se insertan dentro del marco de obligaciones del Estado Mexicano de seguridad pública del artículo 21 constitucional.⁷
15. También se considera superada la segunda grada (idoneidad) porque existe una relación medio-fin entre la creación del PANAUT y el fin que perseguía. Lo anterior, porque la base de datos con información de usuarios, en principio, permitía tener un mayor control sobre el uso de los dispositivos y contrarrestaba la

⁴ "Artículo 16. [...]"

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, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

[...]"

⁵ **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.**

"Artículo 16. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales."

"Artículo 25. El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento."

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

"Artículo 6. Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley."

"Artículo 13. El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable."

⁶ **Convention for the Protection of Individuals with Regard to Automatic Processing of Data – Council of Europe – European Treaty Series No. 108.** Ratificado por México el 28 de junio de 2018, entrada en vigor el 1 de octubre de 2018.

Article 5 – Quality of data

Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

⁷ **Artículo 21.** La investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función.

[...]

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

[...]

barrera del anonimato que da pie a que estos mecanismos sean vistos como herramientas útiles y seguras para la comisión de los delitos. Por lo tanto, el padrón podía servir como un mecanismo inhibitorio para las conductas. Al respecto del análisis de idoneidad, el INAI había señalado que no existe evidencia que demuestre que registros como el PANAUT impactan en la reducción de delitos de extorsión y secuestro. El estudio rechaza este argumento porque considera que: *“el análisis de idoneidad desde un escrutinio ordinario no implica analizar si la medida adoptada por el legislador es la mejor de las medidas posibles, o si es plenamente eficaz para la consecución de la finalidad que persigue.”*⁸ Solamente se debe analizar si existe una relación de instrumentalidad, y si la medida contribuye en *alguna medida* al fin. Es decir, si ésta es *susceptible* de contribuir a la consecución.

16. Finalmente, concluye que no se satisface la tercera grada del test (necesidad), pues existen otras medidas en el ordenamiento jurídico que son igualmente idóneas para el combate de las conductas delictivas y que afectan en menor grado los derechos humanos señalados. Como ejemplos de éstas, señala la intervención de comunicaciones a partir de la autorización de un juez, así como la geolocalización y entrega de datos conservados por los concesionarios de telecomunicaciones.
17. Al no haberse superado la grada de necesidad, considera innecesario que se supere la cuarta grada (proporcionalidad en sentido estricto). Asimismo, considera innecesario realizar la prueba de proporcionalidad en sentido estricto, pues como el PANAUT no es razonable a la luz del escrutinio ordinario, a mayor razón no supera el otro. Por lo tanto, se declara la invalidez de la totalidad del PANAUT.

B. Razones de la concurrencia.

18. Estoy de acuerdo con que el PANAUT no supera la prueba de proporcionalidad, pero considero que esto es porque no supera la grada de idoneidad.
19. La grada de idoneidad presupone la existencia de una relación medio-fin entre la medida que restringe el derecho y el fin que ésta persigue. Para superar la grada, es suficiente que la medida contribuya, en algún modo y grado, a lograr el propósito del legislador. En ese sentido, en aras de la libertad legislativa y como regla general, me parece suficiente observar una relación hipotética entre la medida específica y el resultado esperado. Es decir, mientras se observe una relación lógica entre la medida propuesta por el legislador y la finalidad identificada en la primera grada, se puede considerar que la medida es idónea.
20. Sin embargo, considero que esta regla general debe exceptuarse cuando se cuente con evidencia fuerte y directamente aplicable al caso concreto respecto a la efectividad de la medida. Esa evidencia puede apoyar o, en su defecto, desvirtuar esa relación lógica medio-fin, y demostrar que en realidad la medida no es idónea para alcanzar el fin de la norma.
21. Este me parece que es el caso particular del PANAUT, dado que el padrón tiene un claro predecesor — el RENAUT— que aporta evidencia específica, aplicable directamente a México, de la ineficacia de la medida para alcanzar su objetivo.⁹ Si bien es cierto que el PANAUT no es textualmente idéntico al RENAUT, ambas bases de datos son, en la práctica, casi iguales, y las diferencias son irrelevantes para efectos del análisis aquí presentado.¹⁰

⁸ Párrafo 277 del engrose.

⁹ La ineficacia del RENAUT quedó expresada como la principal razón para su derogación en el proceso legislativo que llevó a su reforma. Asimismo, esto fue recordado y reiterado por diversos expertos participantes del Foro Virtual sobre Registro de Usuarios de Telefonía Móvil realizado durante el proceso legislativo que condujo a la creación del PANAUT, organizado por la Comisión de Comunicaciones y Transportes de la Cámara de Diputados. Véase:

1) La primera iniciativa de reforma que llevó a la derogación del RENAUT: “INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN, ADICIONAN Y DEROGAN DIVERSAS DISPOSICIONES DEL CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES, DEL CÓDIGO PENAL FEDERAL, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y DE LA LEY QUE ESTABLECE LAS NORMAS MÍNIMAS SOBRE READAPTACIÓN SOCIAL DE SENTENCIADOS” *Cámara de Senadores*. 15 de marzo de 2011. Consultable en: <<https://legislacion.scjn.gob.mx/Buscador/Paginas/wfProcesoLegislativoCompleto.aspx?q=Fahf/ZCcCGTRH7BTx0eHtKCK2XcouBu2Gk48zkHs/UVDTxQJtJ8Oy7bbYPGtKQvprSxMylppT7yrvuvbdkaxg==>>>

2) “Foro Virtual sobre Registro de Usuarios de Telefonía Móvil” *Cámara de Diputados*. 30 de noviembre de 2020. Transmitido por: <<https://www.youtube.com/watch?v=ZToTgpeo4Go&t=2110s>>

¹⁰ Para llegar a esta conclusión, se realizó un comparativo de la información contenida en ambas bases de datos, de sus objetivos y de la forma en que éstas operaban. Aunque algunos campos de datos eran distintos y el lenguaje utilizado en la regulación variaba, las diferencias entre el PANAUT y el RENAUT eran menores. En particular, los cambios en el PANAUT no atendían los problemas que fueron identificados en el RENAUT como las razones de su fracaso.

22. El PANAUT pretendía reducir la incidencia delictiva con el argumento de que las autoridades, al contar con los datos personales de los usuarios de telefonía, podían identificar y detener a quienes cometieran delitos utilizando sus teléfonos móviles. Sin embargo, la exposición de motivos de la iniciativa por la que se derogó el RENAUT en 2011 señala justamente a dicho argumento como la principal razón por la que éste fracasó, pues parte de una falsa premisa: que las personas cometiendo los delitos utilizan celulares registrados a su nombre o a nombre de sus cómplices.¹¹
23. La iniciativa que llevó a la derogación del RENAUT también señala que un problema de dicho registro fue que no se podía garantizar la veracidad de los datos.¹² El PANAUT *parecía* abordar este problema al requerir que los usuarios proporcionen sus datos biométricos. Sin embargo, esto no lo soluciona.
24. Para que los datos biométricos pudieran ser útiles para tales efectos, deberían poder cruzarse con un padrón nacional de identidad que ya contara con datos biométricos, pero en México no existe un registro con estas características. Lo más parecido a esto es el padrón electoral del Instituto Nacional Electoral, que únicamente cuenta con el 74%¹³ de la población registrada. Lo que significa que no se podría verificar la identidad de todos los que registran en el PANAUT o, alternatively, se tendría que negar el servicio de telefonía móvil a los ciudadanos que no se encontraran inscritos en el padrón electoral, ciudadanos que tienden a formar parte de la población vulnerable.
25. Más aún, incluso si pudiera garantizarse la veracidad de la información que se registra en el PANAUT, éste seguiría sin ser útil para disuadir a la delincuencia porque podrían seguirse cometiendo delitos utilizando teléfonos registrados a otro nombre, tarjetas SIM del extranjero, o servicios de internet para hacer llamadas telefónicas.¹⁴
26. Por lo tanto, considero que existe evidencia contundente de que el PANAUT no superaba la grada de idoneidad y, por ende, era innecesario analizar si superaba la grada de necesidad del test. Así pues, esto era suficiente para declarar la invalidez total del sistema normativo impugnado.
27. Sin perjuicio de lo anterior, me expresé también de acuerdo con los argumentos esgrimidos en el análisis de la grada de necesidad. Sin embargo, me parece relevante señalar que esto no significa, en ningún sentido, un pronunciamiento respecto de la constitucionalidad (o inconstitucionalidad) de las medidas con las que el PANAUT fue comparado.

Ministro **Juan Luis González Alcántara Carrancá**.- Firmado electrónicamente.- Secretario General de Acuerdos, Licenciado **Rafael Coello Cetina**.- Rúbrica.

EL LICENCIADO **RAFAEL COELLO CETINA**, SECRETARIO GENERAL DE ACUERDOS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN: CERTIFICA: Que la presente copia fotostática constante de seis fojas útiles, concuerda fiel y exactamente con el original firmado electrónicamente del voto concurrente formulado por el señor Ministro Juan Luis González Alcántara Carrancá, en relación con la sentencia del veintiséis de abril de dos mil veintidós, dictada por el Pleno de la Suprema Corte de Justicia de la Nación en 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 y diversos Senadores Integrantes de la LXIV Legislatura. Se certifica con la finalidad de que se publique en el Diario Oficial de la Federación.- Ciudad de México, a siete de noviembre de dos mil veintidós.- Rúbrica.

¹¹ "En gran medida, la incapacidad del RENAUT ha sido producto de la idea de que el registro de usuarios de celulares en una gran base de datos nacional garantizaría la ubicación de los responsables de un delito. Una idea errónea fundada sobre el argumento de que los delincuentes utilizarían aparatos de comunicación móvil registrados a su nombre o a nombre de sus cómplices. La realidad es otra." Véase *supra* pie de página 9.

¹² "Tal como se ha señalado en esta misma tribuna, el registro de un teléfono mediante nombre y Clave Única de Registro de Población (CURP) no garantiza la veracidad de los datos y menos aún que en el caso de cometerse un delito realmente se atrape al culpable; por el contrario, puede culparse a una persona que no lo sea. Asimismo, resulta inoperante la obligación de los concesionarios de verificar la veracidad de la información suministrada pues las compañías operan a través de miles de distribuidores y agentes a los que no puede hacerse responsables de hacerlo." *Idem*.

¹³ 93,210,066 ciudadanos en el padrón electoral (DERFE INE, 2022) / 126,014,024 habitantes en México (INEGI, 2020) = 0.7397
Véase: <<https://www.ine.mx/credencial/estadisticas-lista-nominal-padrón-electoral/>>

¹⁴ Tal como lo advirtieron diversos expertos participantes del foro realizado en el marco de la reforma del PANAUT, organizado por la Comisión de Comunicaciones y Transportes de la Cámara de Diputados. Véase *supra* pie de página 9.

VOTO CONCURRENTE QUE FORMULA EL SEÑOR MINISTRO LUIS MARÍA AGUILAR MORALES, EN RELACIÓN CON LA ACCIÓN DE INCONSTITUCIONALIDAD 82/2021 Y SU ACUMULADA 86/2021.

En sesión celebrada el veintiséis de abril de dos mil veintidós, el Tribunal Pleno de esta Suprema Corte de Justicia de la Nación resolvió en definitiva las acciones de inconstitucionalidad citadas al rubro, promovidas, respectivamente, por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y por una minoría de senadores, en las que se impugnó el Decreto por el cual se reforman y adición diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno.

En su resolución, el Tribunal Pleno de la Suprema Corte de Justicia de la Nación determinó, por un lado, reconocer la validez del procedimiento legislativo de creación del Decreto impugnado y, por otra parte, declarar la invalidez de la totalidad del sistema normativo que integraba dicho Decreto y que tenía por objeto implementar el Padrón Nacional de Usuarios de Telefonía Móvil.

Si bien compartí el sentido de la resolución, en algunos casos lo hice por consideraciones distintas y, en otros, por razones adicionales. Dichas razones son las que motivan la formulación del presente voto concurrente y las cuales manifestaré a continuación.

Considerando Sexto. Violaciones al procedimiento legislativo.

En el estudio de fondo, previo a analizar los conceptos de invalidez destinados a confrontar las normas contenidas en el Decreto impugnado con el parámetro de regularidad constitucional, se analizaron los argumentos encaminados a evidenciar una serie de irregularidades que, a juicio de los Senadores accionantes, se cometieron en su procedimiento de creación.

Por unanimidad de votos, se declararon infundadas las dos líneas argumentativas formuladas en contra del procedimiento legislativo del Decreto impugnado, a saber, la falta de fundamentación y motivación de los dictámenes emitidos tanto por la Cámara de Diputados como por la Cámara de Senadores, así como las violaciones que, a juicio de la minoría parlamentaria del Senado de la República, se cometieron al aprobarse el dictamen por las Comisiones Unidas de Comunicaciones y Transportes de Estudios Legislativos.

Si bien compartí el reconocimiento de validez del procedimiento legislativo impugnado, respecto a la segunda violación alegada, lo hice por consideraciones distintas.

A fin de explicar mi postura, debe tomarse en cuenta que el motivo de impugnación de la minoría parlamentaria, en cuanto a la segunda violación, reposó en el hecho de que el proyecto de dictamen fue votado primero por la Comisión de Comunicaciones y Transportes y después, en una sesión distinta, por la Comisión de Estudios Legislativos, pues en ésta última existió un empate acerca de una reserva presentada por un senador que debía resolverse previamente.

Bajo el dicho de los accionantes, tal actuación constituyó una violación al Reglamento del Senado, conforme al cual los dictámenes producidos bajo la modalidad de trabajo de comisiones unidas deben ser aprobados en ese acto por la mayoría absoluta de los integrantes de cada una de las comisiones que participan, por lo que no resultaba posible que el dictamen fuera votado primero por una Comisión, tomando en cuenta que la reserva que estaba pendiente de resolverse en su homóloga podía influir en el voto del resto de sus integrantes.

A juicio de una mayoría de Ministras y Ministros, dicho planteamiento resultó infundado, pues del Reglamento del Senado no puede desprenderse que las comisiones unidas deban aprobar el proyecto de dictamen en un solo acto o de manera simultánea. Así, se argumentó que lo único que se exige en esos casos es que la aprobación se dé por la mayoría absoluta de los integrantes de las comisiones dictaminadoras, lo cual aconteció en el caso.

Respetuosamente no compartí tal argumentación, pues a mi juicio, resulta contrario a la lógica del trabajo de Comisiones Unidas el que la Comisión de Comunicaciones y Transportes haya votado y aprobado el dictamen estando pendiente la votación en la Comisión de Estudios Legislativos sobre las reservas presentadas, pues si bien en el Reglamento del Senado no existe una regla específica que resuelva esa circunstancia, es decir, una previsión que ordene suspender la votación de una de las Comisiones hasta en tanto la otra resuelva sobre un punto sobre el que no hay acuerdo, me parece que derivado de la naturaleza del trabajo en comisiones unidas, cuando exista un empate en una de ellas, su homóloga sí debe esperar a que se resuelva ese punto, sobre todo si el resultado de dicha votación puede implicar que ciertas cuestiones se discutan antes de presentar el dictamen correspondiente al Pleno del Congreso correspondiente.

A mi parecer, esa interpretación es la que más resulta acorde a la luz de la deliberación pública que debe estar presente en la etapa de dictaminación por parte de las Comisiones legislativas.

Pese a lo anterior, considero que en este caso en específico, tal situación no tiene el potencial de invalidar todo el procedimiento legislativo del Decreto impugnado, pues si bien no obra constancia alguna de la que pueda desprenderse la votación definitiva de la Comisión de Estudios Legislativos sobre las reservas presentadas, al final de cuentas, en la página del Senado sí obra constancia de que en la sesión de la Comisión de Estudios Legislativos existió mayoría de votos a favor del Dictamen correspondiente, por lo que puede presumirse que una vez realizada la votación que se encontraba pendiente, aquella no reunió la mayoría para poder admitir las reservas desde ese momento.

Así, contrario a la posición mayoritaria, considero que lo infundado del argumento radica en que, pese a que la actuación de las comisiones dictaminadoras sí fue, en principio, contraria a la lógica del trabajo de Comisiones Unidas, lo cierto es que en este caso y por las particularidades que ya manifesté, tal violación no tiene el potencial invalidante para *viciar* todo el procedimiento legislativo del Decreto combatido.

Considerando Séptimo. Vulneración a los derechos de privacidad, intimidad y protección de datos personales.

Finalmente, en el estudio de la regularidad constitucional del Decreto combatido, y después de realizar tanto un escrutinio estricto como ordinario, el primero para analizar las intromisiones a la intimidad y protección de datos sensibles y el segundo para analizar las injerencias al derecho a la privacidad y la protección de datos personales, se concluyó que las normas impugnadas son inconstitucionales, pues en el sistema jurídico mexicano ya existen mecanismos igualmente idóneos para lograr los fines que se pretendían con el Padrón Nacional de Usuarios (en general, colaborar con las autoridades de justicia en relación con la comisión de delitos, especialmente de los cometidos mediante el uso de telefonía celular) y que restringen en menor medida los derechos en cuestión.

Si bien compartí la conclusión adoptada, así como sus consideraciones, me permitiré exponer algunas razones adicionales que, a mi parecer, refuerzan la inconstitucionalidad detectada.

Como punto de comienzo, me parece importante partir de la utilidad que se buscó imprimir con la nueva normatividad que regulaba el Padrón Nacional de Usuarios de Telefonía Móvil, lo cual obliga a tener presente que, desde su expedición, y hasta la fecha, la Ley Federal de Telecomunicaciones y Radiodifusión establece diversas obligaciones a cargo de los concesionarios en materia de seguridad y justicia. Entre dichas obligaciones se encuentra la de conservar un registro y control de comunicaciones que se realicen desde cualquier línea, bajo cualquier modalidad y que permita identificar, entre otros datos, el nombre, denominación o razón social, así como el domicilio del suscriptor¹.

No obstante, si bien en términos de la legislación vigente esos datos deben recabarse *bajo cualquier modalidad*, en los “*Lineamientos de Colaboración en Materia de Seguridad y Justicia*” emitidos por el Instituto Federal de Telecomunicaciones y Radiodifusión, se dispone que en relación con los datos indicados en el artículo 190, fracción II, de dicho ordenamiento, tratándose del servicio móvil, el nombre y domicilio del usuario, sólo deberá recabarse en la modalidad de pospago², sin que sea necesario el registro de tales datos cuando se opte por la modalidad de prepago.

De esta forma, a la fecha, los concesionarios se mantienen obligados a recabar, conservar y, en dado caso, entregar ciertos datos, tales como el nombre, denominación o razón social y domicilio del suscriptor; sin embargo, dicha obligación se encuentra limitada a los casos en que se opte por la modalidad de pospago, pues así se dispone en los Lineamientos referidos y que a la fecha no han sido derogados; máxime que en el aspecto resaltado desarrollan reglas que continúan vigentes.

¹ “**Artículo 190.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

(...)”

II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

a) Nombre, denominación o razón social y domicilio del suscriptor;

(...)”.

² “**Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996**” publicado en el Diario Oficial de la Federación el 2 de diciembre de 2015.

“**DÉCIMO CUARTO.** El sistema o sistemas utilizados para el registro de datos de comunicaciones de líneas privadas y líneas de los servicios fijo y móvil deberán contar con la capacidad de almacenar y entregar los datos indicados en la fracción II del artículo 190 de la LFTR.

(...)”

III. Para el servicio móvil en las modalidades de prepago y pospago se registrará y conservará la información correspondiente a:

a) **Nombre y dirección del usuario registrado, en el caso de la modalidad de pospago;**

(...)”

IV. En el caso de la modalidad de prepago, se registrarán y conservarán además los datos que permitan identificar:

a) El lugar, fecha y hora en la que se realizó la compra del dispositivo de prepago y/o la tarjeta SIM, en el caso en que el Concesionario o Autorizado los comercialice por canales propios, o

b) En su caso, los datos del distribuidor al que le fue entregado el dispositivo de prepago o la tarjeta SIM para su comercialización.

(...)” (énfasis añadido).

Esto resulta de suma relevancia para este asunto, tomando en cuenta que en el proceso legislativo del Decreto impugnado³, se expresó que derivado de su *fácil adquisición* y por los *nulos requisitos para la obtención y registro de un plan de telefonía, la delincuencia ha optado por el servicio de prepago* en el que prevalece el anonimato, pues no se puede saber quiénes adquirieron el número a través del cual se cometen delitos, lo que incluso ha impedido que las autoridades rastreen su geolocalización, al ser común que los equipos sean desechados después de su uso.

Para solucionar ese problema, y con el *único fin de colaborar con* las autoridades en materia de seguridad y justicia, el Congreso de la Unión consideró necesaria la existencia de una “única” base de datos, distinta a la que debe mantener cada concesionario y que concentre información de todos los usuarios de cada línea telefónica móvil, quienes deberán proporcionar su identificación oficial, comprobante de domicilio y sus datos biométricos, para la activación del servicio de la línea telefónica⁴.

En este contexto, el problema detectado por el legislador federal y su correlativa solución, centra las miradas en el anonimato que se encuentra presente en la modalidad de prepago, circunstancia que resulta de la mayor trascendencia en el ámbito de la seguridad pública, tomando en cuenta que ha sido un factor en la impunidad de los delitos cuya comisión involucra el uso de un teléfono móvil.

Ahora bien, también coincidí en que por el contenido del Decreto impugnado, su análisis debe efectuarse a la luz tanto de un escrutinio ordinario como de uno de carácter estricto, pues entre los distintos tipos de datos que se obliga a los usuarios a proporcionar para la activación del servicio en línea, se encuentran tanto datos personales como datos personales sensibles, los cuales no son tratados de la misma manera en el campo legislativo, por lo que tampoco deben serlo en sede judicial.

En efecto, en términos de la normatividad impugnada, la persona se encuentra obligada a proporcionar su nombre y domicilio, los cuales han sido catalogados por el Instituto Nacional de Acceso a la Información como *datos personales*⁵, pero también sus datos biométricos, los cuales han sido definidos por dicho Instituto como las “*propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona*” y que son medibles, universales, únicos, y permanentes, tales como, por ejemplo, la huella digital, el rostro, la retina, el iris, la geometría de la mano o de los dedos e incluso el ADN⁶, por lo que sin duda alguna deben catalogarse como *datos personales sensibles* en términos de la definición que sobre dicho concepto se ofrece en la Ley General de la materia, en tanto que podrían en última instancia revelar información genética del individuo⁷.

Tomando en cuenta lo anterior, la perspectiva a la luz de la cual debe abordarse el examen en este asunto no puede ser una sola, es decir, no debe analizarse con el mismo rigor la recopilación y acceso de los datos personales, a aquella que se haga sobre los datos biométricos, como datos personales sensibles, pues éstos son los que se refieren a la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un grave riesgo para éste. Además, como se señala en la sentencia, en la acción de inconstitucionalidad 21/2013, se analizó una norma que regulaba la prueba de ADN para identificar testigos a la luz de un escrutinio estricto, sobre lo cual estuve a favor.

Ahora bien, en la aplicación del escrutinio ordinario, compartí que la medida persigue una finalidad constitucionalmente válida, pues busca dotar a las autoridades de una herramienta para un problema no solucionado⁸, como lo es la comisión de delitos en los que se utiliza la telefonía móvil, lo que se inserta en el marco de las obligaciones en materia de seguridad pública que derivan del artículo 21 de la Constitución Federal.

³ Dictamen de las Comisiones Unidas de Comisiones y Transportes y de Estudios Legislativos del Senado de la República, páginas 15 y 16.

⁴ En términos del artículo 180 Quáter de la ley impugnada.

⁵ “Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares” Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Junio de 2016, p.3

⁶ “Guía para el Tratamiento de Datos Biométricos”, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Marzo 2018, página 9.

⁷ “Artículo 3. Para los efectos de la presente Ley se entenderá por:

(...)

X. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, **información genética**, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

(...).”

⁸ Uno de los delitos cometidos con teléfonos móviles es la extorsión. De acuerdo con la **Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública de 2020 y 2021**, en 2019 se cometieron 4.6 millones de delitos de extorsión (en el 88.9% de los casos fue vía telefónica) y en el 2020 dicha cifra aumentó pues se registraron 4.7 millones de delitos de extorsión (en el 90.7% de los casos fue vía telefónica). **En ambos años, el delito de extorsión ocupó el tercer lugar en la lista de los delitos más cometidos en el año** (en el 2019 representaron el 15.3% del total de delitos cometidos, mientras que en el 2020 el 16.9%).

También resulta idónea para lograr dicha finalidad, pues si en esta etapa tan sólo debe analizarse si la medida contribuye *en algún modo y en algún grado* al propósito buscado, el Padrón Nacional de Usuarios, en tanto su objeto es la identificación de cada uno de los usuarios de telefonía móvil, en principio sí contribuye a contrarrestar el anonimato aludido, además de ofrecerle a la autoridad una herramienta adicional para tener mayor información sobre los delitos cometidos bajo esa modalidad.

No dejo de advertir que la persona que utiliza un teléfono móvil para cometer un delito, no necesariamente será la misma que aparece como su titular, pudiéndose así frustrar el objetivo del Padrón y que, además, su eficacia también podría verse disminuida por la situación de personas que no se encuentren registradas en su país de nacimiento o residencia, o que estén en situación de calle, y que, por tanto, no podrían presentar una identificación oficial o proporcionar un comprobante de domicilio.

Adicionalmente, también tengo presente que la medida busca lograr, en esencia, lo que se pretendía con el anterior Registro Nacional de Usuarios de Telefonía Móvil⁹, el cual fue eliminado debido a que se consideró ineficiente para combatir el fenómeno delictivo¹⁰.

Pese a esas circunstancias que podrían obstaculizar la eficacia del Padrón, y aun cuando en esta grada del test resulta posible apoyarse en *convicciones sociales generalmente aceptadas*¹¹, no me parece que exista una evidencia incontrovertible sobre la que podamos considerar que el tener un registro de los usuarios de telefonía móvil en nada coadyuva con el anonimato que existe en la comisión de delitos que utilizan un aparato celular.

No obstante, la medida no resulta necesaria para lograr el fin buscado, pues en nuestro sistema existen diversos mecanismos que le ofrecen a la autoridad vastas herramientas para investigar y, en su caso, perseguir con éxito, los delitos cuya comisión requiere un teléfono móvil, los cuales restringen en menor medida los derechos humanos en cuestión.

Ahora bien, no dejo de observar que los mecanismos expuestos en la sentencia, previstos en la Ley Federal analizada y en el Código Nacional de Procedimientos Penales, como la intervención de comunicaciones, extracción de información, la localización geográfica en tiempo real y la entrega de datos conservados por los concesionarios, no tienen como fin primordial la individualización del usuario que compró el dispositivo, sino la identificación y ubicación de las líneas utilizadas en la comisión de los delitos y que, por tanto, su desahogo, en sí mismo, podría no subsanar, en automático, el problema de anonimato aludido por el legislador.

Sin embargo, tomando en cuenta la información valiosa que puede obtenerse por medio de ellos, referida no sólo a la ubicación de los equipos relacionados con los hechos que se investigan, sino también al contenido mismo de la comunicación, su correcto desahogo sí puede arrojar *indicios* sobre la persona que cometió el delito; la cual, insisto, no necesariamente es quien compró el dispositivo utilizado.

De esta manera, el no tener certeza sobre quién es el titular de la línea, no impide que la investigación y persecución penal, en su caso, culmine con un resultado exitoso, ya que la información que puede obtenerse con los mecanismos expuestos en el proyecto, relacionada con otra a la que, en su caso, podría accederse en el marco de una investigación, genera que el anonimato no sea una condicionante para el éxito de la investigación y, en su caso, persecución de un delito.

Lo que demuestra que la obligación de todos los usuarios de proporcionar cierta información referida a su identidad es una medida que no es estrictamente necesaria para lograr el fin buscado, pues en el sistema jurídico mexicano ya existen mecanismos que bien utilizados pueden tener como resultado final, no la identificación del titular de la línea, sino de quién cometió el delito en cuestión, que es, al final de cuentas, lo que realmente va a coadyuvar a la seguridad pública de la población.

Asimismo, tales medidas restringen en menor medida los derechos en cuestión porque, como se señala en la sentencia, además de que para su acceso se requiere autorización judicial, están sujetos a una temporalidad específica y no se traducen en una recopilación generalizada que abarca a la mayoría de la población mexicana.

⁹ El cual ordenaba que los concesionarios llevaran un registro y control de sus usuarios tanto en la modalidad de líneas contratadas en plan tarifario como en líneas de prepago, el cual debía contener, entre otros datos, el nombre completo, domicilio, nacionalidad y la toma de impresión de huella dactilar de la persona.

¹⁰ En una de las iniciativas presentadas para derogar el Registro Nacional se manifestó que no rindió frutos en la prevención, investigación y persecución de delitos, pues el registro de un teléfono no garantiza la veracidad de los datos; no hay incentivos para que las personas mantengan los datos registrados e **incluso incentiva el robo de equipos**. Consultado en la siguiente liga: <https://legislacion.scjn.gob.mx/buscador/paginas/wfProcesoLegislativoCompleto.aspx?q=BHGCBwRG7ukiUiW/WEu/mX+grKuyYUL3tMCZY2Vr7S/HRU927iA19aLghBPAOX7hmTX1EscdlD3x/nmd2Nlvg==>

¹¹ En términos de la tesis 1a. CCLXVIII/2016 (10a.), de rubro: **"SEGUNDA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA IDONEIDAD DE LA MEDIDA LEGISLATIVA."** Registro 2013152; Primera Sala; [TA]; 10a. Época; Gaceta del S.J.F.; Libro 36, Noviembre de 2016, Tomo II, pág. 911.

Todo lo anterior me lleva, lógicamente, a considerar que la vulneración al derecho a la intimidad y la protección de datos sensibles tampoco supera el escrutinio estricto de proporcionalidad.

Ahora bien, es cierto que con lo dicho me resulta suficiente para evidenciar la inconstitucionalidad del sistema normativo impugnado; sin embargo, también es cierto que al ser el test de proporcionalidad, ya sea ordinario o estricto, una herramienta argumentativa, no existe un impedimento técnico para que puedan emitirse pronunciamientos adicionales, siempre y cuando refuercen la inconstitucionalidad de la medida.

Por ese motivo, y tomando en cuenta la particular relevancia que presenta este asunto, me parece importante evidenciar el desequilibrio entre la intensa afectación al derecho de privacidad, intimidad y protección de datos personales y sensibles, frente al grado en que podrían satisfacerse los fines legislativos a través de la creación del Padrón Nacional de Usuarios de Telefonía Móvil.

Esto, pues si bien considero que tal medida contribuye positivamente a la realización del fin que persigue, también expuse ciertos argumentos que demuestran cómo ciertas circunstancias, muy factibles de ocurrir, pueden frustrar de manera importante la eficacia del Padrón Nacional, como la utilización de equipos móviles robados para la comisión de delitos e incluso la imposibilidad de ciertas personas de registrarse ante el Padrón, al no contar con un domicilio e incluso en otros casos con una identificación que permita dar fe de su identidad, propiciando así eventualmente el uso de un teléfono móvil que no se encuentre registrado a su nombre.

En contraste con ello, se ubica la intensa afectación al derecho de privacidad, intimidad y protección de datos personales y datos personales sensibles, pues con motivo del Decreto impugnado, cualquier persona que quisiera tener un teléfono móvil se encontraría obligada a proporcionar información tan delicada que es apta de reflejar tanto sus aspectos físicos como genéticos.

Tomando en consideración lo anterior, la intensa afectación a los derechos en cuestión se demuestra tomando en cuenta, por un lado, que aun cuando la legislación señale que la información del Padrón sería *confidencial* y *reservada*, lo cierto es que se permite su acceso tanto a los concesionarios como al propio Estado a través del Instituto Federal de Telecomunicaciones y Radiodifusión, así como a cualquier autoridad *de seguridad de procuración y administración de justicia* que cuente con facultades para ello, sin necesidad de contar con una autorización judicial y la cual, bajo mi criterio, es necesaria en cualquier técnica de investigación que, como el Padrón Nacional, sea susceptible de afectar a los derechos humanos en un grado significativo o difícilmente reparable.

Y, por otra parte, porque como fue resuelto en la acción de inconstitucionalidad 10/2014 y su acumulada 11/2014, al analizar la norma impugnada que regulaba la figura de la geolocalización, el acceso a la información del Padrón Nacional no se prevé como una medida que opere en supuestos o casos excepcionales, por lo que incluso se permite en delitos menores o que no pongan en alto riesgo la vida, integridad y la seguridad de la persona¹², pero más grave aún, su acceso por parte del Estado se prevé como condicionante para acceder al servicio de telefonía móvil, por lo que operaría incluso en supuestos en los que la persona ni siquiera se encuentre relacionada con la investigación de algún hecho delictivo.

Además, de cara a los posibles obstáculos que podrían impedir una plena consecución de los fines propuestos por el legislador, se encuentra también la intensa afectación que un sector de la población sufrirá en el ejercicio de sus derechos de acceso a la información y libertad de expresión, entre otros, pues el registro en el Padrón Nacional –y, por tanto, la obligación de contar con ciertos datos, incluidos un domicilio– se traduciría en una condicionante para contar con un teléfono móvil; y el cual, en nuestro país, es utilizado por la mayoría de las personas para tener acceso a internet.

En efecto, en la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares¹³, realizada por el Instituto Nacional de Estadística y Geografía, en colaboración con la Secretaría de Comunicaciones y Transportes y el Instituto Federal de Telecomunicaciones, se expuso que, en el 2020, el 72% de la población de 6 años o más son usuarios de internet, a la cual tienen acceso, el 96% de ella, a través de un celular inteligente. Asimismo, se señaló que entre las principales actividades que realizan se encuentran la de comunicarse (en un 93.8%), buscar información (en un 91%) y acceder a redes sociales (ello en un 89%).

¹² Al resolver la acción de inconstitucionalidad 10/2014 y su acumulada 11/2014, por mayoría de 8 votos se declaró la invalidez del artículo 303 del Código Nacional de Procedimientos Penales que regulaba la figura de geolocalización (antes de su reforma de 17 de junio de 2016).

¹³ Consultable en la siguiente página: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf

La importancia del acceso a internet ha sido debidamente explicada en los “Estándares para una Internet libre, abierta e incluyente” aprobados por la Comisión Interamericana de Derechos Humanos, pues en ellos se manifestó que el acceso a internet, hoy en día, constituye una condición *sine qua non* para el ejercicio efectivo de los derechos humanos, especialmente los de libertad de expresión, asociación y reunión, educación, salud y cultura; y que, su falta de acceso, incrementa la vulnerabilidad y profundiza la desigualdad, perpetuando la exclusión de muchos¹⁴.

Además, por su importancia, se consideró que la aplicación de sanciones negando el acceso a internet, como en este caso puede ocurrir para un 96% de los usuarios que acceden a ella a través de un celular, sólo podrá justificarse cuando dichas sanciones cumplan, entre otros, con los requisitos de legalidad, proporcionalidad y necesidad en una sociedad democrática¹⁵.

Si bien mi intención no es la de desarrollar de manera exhaustiva el test de proporcionalidad a la luz de los diversos derechos humanos que también se ven restringidos por el Decreto impugnado, sí me parece importante resaltar la afectación que podría resentir una persona que no pueda registrarse ante el Padrón, lo que a mi juicio, confirma la inconstitucionalidad de la medida.

Por último, me parece sumamente enriquecedor e importante que en la sentencia se retome el análisis efectuado en el “Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión” de veintidós de mayo de dos mil quince, pues, en efecto, en él se consideró que el registro obligatorio de las tarjetas SIM, además de que puede proporcionar a los gobiernos la capacidad de vigilar a las personas y periodistas más allá de cualquier interés legítimo, menoscaban directamente el anonimato, en particular para aquellas personas que acceden a internet únicamente a través de la tecnología móvil y el cual, junto con el cifrado, brindan a los individuos una zona de vida privada para sostener opiniones y ejercer su libertad de expresión sin injerencia y ataques arbitrarios o ilegales¹⁶, por lo que entre las recomendaciones dirigidas a los Estados se encuentra la de abstenerse de *obligar a los usuarios de los teléfonos móviles que registren su tarjeta SIM*¹⁷.

Sin duda alguna falta un largo camino por recorrer para que la seguridad en México deje de ser vista como un objetivo utópico o imposible de alcanzar y que, en ese sentido, es necesario y obligatorio que todas las autoridades, en el ámbito de su competencia, implementen medidas o acciones que se encuentren dirigidas a acercarnos, cada vez más, al Estado al que todos aspiramos convertirnos.

Sin embargo, también es necesario que en ese camino no se inobserven o restrinjan, de manera injustificada, los derechos humanos de las personas, pues buscando la consecución de un fin primordial desde el punto de vista constitucional, como lo es la seguridad de la población mexicana, a costa de sus derechos, sería como condenar la medida implementada desde su inicio.

En mérito de las razones expuestas, sirvan estas líneas para expresar mi respetuoso disenso en relación con algunas consideraciones de esta ejecutoria y algunos motivos adicionales en relación con ciertas consideraciones de esta ejecutoria.

Ministro **Luis María Aguilar Morales**.- Firmado electrónicamente.- Secretario General de Acuerdos, Lic. **Rafael Coello Cetina**.- Firmado electrónicamente.

EL LICENCIADO **RAFAEL COELLO CETINA**, SECRETARIO GENERAL DE ACUERDOS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN: CERTIFICA: Que la presente copia fotostática constante de ocho fojas útiles, concuerda fiel y exactamente con el original firmado electrónicamente del voto concurrente formulado por el señor Ministro Luis María Aguilar Morales, en relación con la sentencia del veintiséis de abril de dos mil veintidós, dictada por el Pleno de la Suprema Corte de Justicia de la Nación en 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 y diversos Senadores Integrantes de la LXIV Legislatura. Se certifica con la finalidad de que se publique en el Diario Oficial de la Federación.- Ciudad de México, a siete de noviembre de dos mil veintidós.- Rúbrica.

¹⁴ “Estándares para una Internet libre, abierta e incluyente”, Correspondiente al Capítulo III del Informe Anual 2016 de la Relatoría Especial para la Libertad de Expresión, aprobado el 15 de marzo de 2017 por la Comisión Interamericana de Derechos Humanos, p. 20.

¹⁵ *Idem*, p. 22.

¹⁶ Asamblea General de las Naciones Unidas, “Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye” 22 de mayo de 2015, párrafos 9, 16 y 51.

¹⁷ *Ibidem*, párr. 60.

VOTO CONCURRENTES QUE FORMULA EL MINISTRO PRESIDENTE ARTURO ZALDÍVAR LELO DE LARREA EN 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 Y DIVERSOS SENADORES INTEGRANTES DE LA LXIV LEGISLATURA.

En sesiones de veinticinco y veintiséis de abril de dos mil veintidós, el Tribunal Pleno de la Suprema Corte de Justicia de la Nación resolvió 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 y diversos Senadores integrantes de la LXIV Legislatura, respectivamente, en la cual se declaró la invalidez de la totalidad del sistema normativo que integra el Decreto de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión publicado en el Diario Oficial de la Federación el dieciséis de abril de dos mil veintiuno.

Lo anterior, pues se estimó que el Padrón Nacional de Usuarios de Telefonía Móvil (en adelante “PANAUT”) debería analizarse como un sistema y someterse a un test ordinario y a un test estricto de proporcionalidad, para concluir que las disposiciones que integraban el Decreto impugnado no los superaban, por lo que afectaban de manera desproporcionada los derechos fundamentales a la privacidad, intimidad y protección de datos personales.

Ahora bien, aun cuando comparto la invalidez de las normas impugnadas por constituir medidas que interfieren de manera desproporcionada en los derechos fundamentales antes mencionados, lo cierto es que formulo el presente voto concurrente con la finalidad de puntualizar algunos aspectos que, desde mi perspectiva, fortalecerían la doctrina que esta Suprema Corte ha construido tratándose de los derechos a la privacidad, intimidad y protección de datos personales.

En ese sentido, dividiré mi voto en dos apartados, en el primero, me referiré a las consideraciones que sustentaron la decisión de la sentencia en su estudio de fondo; mientras que, en el segundo, me ocuparé de exponer las razones que considero robustecen la inconstitucionalidad de las normas impugnadas y que abonan en la construcción jurisprudencial de los derechos antes mencionados.

I. Criterio adoptado por el Tribunal Pleno.

En el considerando séptimo, denominado “Vulneración a los derechos de privacidad, intimidad y protección de datos personales”, se decidió declarar la invalidez del Decreto controvertido, en virtud de que se vulneran, por un lado, los derechos a la privacidad y a la protección de datos personales y, por el otro, los derechos a la intimidad y a la protección de datos sensibles.

Así, se concluyó que las normas en estudio transgreden el derecho fundamental a la privacidad y protección de datos en general, al no superar un test de escrutinio ordinario en su grado de necesidad, debido a que existen medidas igualmente idóneas que el PANAUT, pero menos restrictivas a esos derechos, tales como son la intervención de comunicaciones, la geolocalización y la entrega de datos conservados por los concesionarios de telecomunicaciones o autorizados, así como la cancelación de señales de telefonía celular dentro del perímetro de establecimientos penitenciarios y los estudios para inhibir y combatir el uso de telecomunicaciones en la comisión de delitos.

Asimismo, se decidió que para determinar lo referente a la afectación al derecho a la intimidad y la protección de datos sensibles no era necesario agotar la metodología que se propone para un test de escrutinio estricto, pues el PANAUT instituye un mismo régimen normativo tanto para la información privada y datos personales como para la información íntima y datos sensibles, por lo que si ya se demostró que las normas no superan un test ordinario, era claro que tampoco superarían un escrutinio estricto.

Adicionalmente se sostuvo que, el Decreto impugnado no preveía mecanismos de protección para el PANAUT, conforme a los principios cinco y seis del Comité Jurídico Interamericano¹, relativos a la Confidencialidad y Seguridad de los Datos, incorporados en los artículos 31 a 42 de la Ley General de

¹ **Principios Actualizados sobre la Privacidad y la Protección de Datos Personales adoptados por el Comité Jurídico Interamericano (CJI) y aprobados por la Asamblea General de la OEA en 2021.**

Principio Cinco: Confidencialidad.

Los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley.

Principio Seis: Seguridad de los Datos.

La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aún cuando éstos ocurran de manera accidental. Dichas salvaguardias deberían ser objeto de auditoría y actualización permanente.

Protección de Datos Personales en Posesión de Sujetos Obligados. Por último, se precisó que en la emisión del Decreto impugnado se omitió realizar la Evaluación de impacto en la protección de datos personales, a que se refiere el diverso 74 de la citada Ley General².

II. Consideraciones adicionales de inconstitucionalidad del Decreto por el que se crea y regula el PANAUT.

Como señalé anteriormente, el propósito del presente voto es para expresar mi coincidencia con la sentencia aprobada por el Pleno de esta Suprema Corte de Justicia de la Nación, en cuanto a la inconstitucionalidad del sistema que integra el Decreto impugnado; sin embargo, como anuncié en la sesión en que se analizó éste, estimo que existen razones adicionales de inconstitucionalidad que impactan en la regulación total del PANAUT, por lo que a partir de ellas también podría haberse declarado la invalidez del Decreto impugnado.

Así, desde mi perspectiva, más que dos niveles de escrutinio –uno ordinario y otro estricto– debe partirse de dos niveles de análisis, pues una cuestión es si la creación de una base de datos con las características del PANAUT supera un test de proporcionalidad, dada su evidente incidencia en los derechos a la privacidad y a la protección de datos personales y otra es si algunos aspectos de esta regulación son inconstitucionales.

Esto es, si el establecimiento de una base de datos de usuarios de telefonía móvil fuera constitucionalmente válida, en el siguiente paso habría que analizar algunos de sus aspectos concretos para ver si dentro de esa regulación hay medidas que resultan inconstitucionales conforme al estándar de escrutinio aplicable.

A partir de lo anterior, como anticipé, es que coincido con la sentencia, pues el análisis que realizó se centró en el primero de los problemas que se nos plantearon; no obstante, tal como se encuentra integrado el Decreto impugnado, podría haberse analizado si algunos aspectos totales de la regulación del PANAUT también son inconstitucionales.

Consecuentemente, el presente voto lo centraré en expresar las razones por las cuales estimo que son inconstitucionales las disposiciones que regulan la recopilación de datos biométricos en bases de datos masivas y a los requisitos para el acceso a los datos del PANAUT.

a) Recopilación de datos biométricos en bases de datos masivas.

La fracción VI del artículo 180 Ter de la Ley Federal de Telecomunicaciones y Radiodifusión³ establece la obligación a los usuarios de telefonía móvil de otorgar sus datos biométricos⁴ para la inscripción en este Padrón Nacional. La relevancia de lo anterior radica en que las tecnologías biométricas *analizan características físicas, fisiológicas o conductuales de una persona con el fin de identificarla*. Por ello, son utilizadas por un gran número de actores gubernamentales con varios objetivos, como la protección de la seguridad nacional.

En ese sentido, me parece significativo hacer notar que su empleo incide en el derecho a la privacidad y la protección de los datos, por lo que tiene, además, el potencial de afectar la libertad de expresión, el acceso a la información y los derechos de asociación e igualdad⁵, dada la relación indisoluble entre ellos⁶.

² **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**

Artículo 74. Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto o los Organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

El contenido de la evaluación de impacto a la protección de datos personales deberá determinarse por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

³ **Ley Federal de Telecomunicaciones y Radiodifusión**

Artículo 180 Ter. El Padrón Nacional de Usuarios de Telefonía Móvil contendrá, sobre cada línea telefónica móvil, la información siguiente:

[...]

VI. Datos Biométricos del usuario y, en su caso, del representante legal de la persona moral, conforme a las disposiciones administrativas de carácter general que al efecto emita el Instituto...

⁴ Los **datos biométricos** son la información personal que se desprende del uso de procesos tecnológicos sobre las características físicas, fisiológicas o conductuales de un individuo y que permiten identificarlo. Estos datos modifican la relación entre cuerpo e identidad porque transforman características del cuerpo humano en datos legible por máquinas para su uso posterior. Las tecnologías biométricas se refieren a aquellas que analizan las características humanas, como el DNA, las huellas dactilares, los patrones de voz, el iris o la retina ocular. De manera más reciente, incluyen mecanismos de reconocimiento facial, biométrica conductual, etc.

Article 19, When bodies become data: Biometric technologies and freedom of expression 2021, página 8, consultado en <https://www.article19.org/wp-content/uploads/2021/04/A19-Biometric-technologies-and-FoE-Policy-2021.pdf>.

⁵ Ídem, páginas 11 a 13.

⁶ **“El derecho humano a la privacidad, según el cual nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley contra esas injerencias, y reconociendo que el ejercicio del derecho a la privacidad es importante para materializar el derecho a la libertad de expresión y para abrigar opiniones sin interferencias, y es una de las bases de una sociedad democrática”.**

AGONU, Resolución aprobada por la Asamblea General el dieciocho de diciembre de dos mil trece, (21 de enero de 2014) A/RES/68/167, página 1, consultado en: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/50/PDF/N1344950.pdf?OpenElement>.

En efecto, la privacidad es necesaria para la materialización de la comunicación de ideas, incluso, actualmente se reconoce el importante papel del anonimato para su ejercicio, lo que se advierte claramente en el caso de las redes sociales⁷, que son un espacio en donde esto puede potencializarse.

Así, aunque el uso de datos biométricos se ha analizado principalmente tratándose de sistemas de vigilancia, la existencia de bases de datos con información biométrica también conlleva el riesgo de lesionar varios derechos.

Al respecto, el Alto Comisionado de la ONU ha manifestado su preocupación respecto al almacenamiento de datos biométricos a gran escala, como en el presente caso. El robo de estos datos es muy difícil de reparar y puede afectar gravemente los derechos humanos de las personas. Además, pueden utilizarse para fines distintos de aquellos para los que fueron recopilados, como el seguimiento y la vigilancia ilegales de personas. Teniendo en cuenta estos riesgos, recomienda que solo se utilicen estas políticas cuando los Estados puedan demostrar que son necesarios y proporcionales para lograr un fin legítimo⁸.

Ahora bien, entre la gama de datos personales, existe una dicotomía entre aquellos que deben considerarse como sensibles y los que no lo son. De ahí se parte para reconocer que el tratamiento de datos personales impacta de distinta manera en la vida privada de las personas, pues puede implicar riesgos y afectaciones de mayor envergadura para los derechos de las personas. Por tanto, el grado de sensibilidad influye en la decisión sobre el nivel de seguridad que se establece para controlar el acceso a dicha información.

Conforme a lo anterior, debe tenerse en cuenta que los datos biométricos se han categorizado como información personal sensible. Así, en los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales del Comité Jurídico Interamericano de la OEA se precisa que dichos datos merecen una protección especial, por los graves perjuicios que podría ocasionar su manejo o divulgación indebida. En esa misma línea, tanto el Reglamento Europeo General de Protección de Datos⁹, como el Convenio para la Protección de las Personas con respecto al Tratamiento de Datos Personales¹⁰ establecen una protección especial para los datos biométricos que identifiquen de manera única a una persona. A nivel nacional, esta información encuadra en la definición de datos sensibles prevista en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados¹¹.

⁷ "Se ha reconocido el importante papel que desempeña el anonimato para salvaguardar y promover la privacidad, la libertad de expresión, la rendición de cuentas política, y la participación y el debate públicos [...] Algunos Estados ejercen una presión significativa contra el anonimato, tanto en el mundo virtual como en el real. Con todo, como el anonimato facilita la opinión y expresión de manera significativa en la red, los Estados deberían protegerlo y no restringir por norma general las tecnologías que lo procuran".

Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión A/HRC/29/32, aprobado por el Consejo de Derechos Humanos de la Asamblea General de las Naciones Unidas en su 29º periodo de sesiones, párrafo 47, consultable en <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/88/PDF/G1509588.pdf?OpenElement>.

Relatora Especial sobre la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, comunicado de prensa R 17/2015, consultado en <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=979&IID=2>.

También, la Suprema Corte Norteamericana ha sostenido que "Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment".

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995); párr. 342.

⁸ ACNUDH, El derecho a la privacidad en la era digital, Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, (3 de agosto de 2018), A/HRC/39/29, párrs. 14 y 61, consultado en: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/61/PDF/G1823961.pdf?OpenElement>

⁹ **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO** de veintisiete de abril de dos mil dieciséis relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales (...).

¹⁰ **Convenio para la Protección de las Personas con respecto al Tratamiento de Datos Personales.**

Artículo 6 – Categorías especiales de datos.

1. El tratamiento de: datos genéticos; datos personales relacionados con delitos, procesos penales y sentencias penales de condena, y medidas de seguridad relacionadas; datos biométricos que identifican únicamente a una persona; datos personales por la información que revelan en relación con los orígenes raciales o étnicos, opiniones políticas, afiliaciones sindicales, creencias religiosas u otras, salud o vida sexual, estará permitido únicamente cuando se consagren garantías apropiadas conforme a la ley, complementando aquellas del presente Convenio.

2. Dichas garantías deberán proteger de los riesgos que el tratamiento de datos sensibles podría presentar para los intereses, derechos y libertades fundamentales del titular de datos, particularmente el riesgo de discriminación".

¹¹ **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Artículo 3.** Para los efectos de la presente Ley se entenderá por:

[...]
X. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual...

Por ello, considero que la fracción VI del artículo 180 ter de la Ley Federal de Telecomunicaciones y Radiodifusión que obliga a los usuarios de telefonía móvil a otorgar sus datos biométricos para su inscripción en el PANAUT debe ser sometida a un *escrutinio estricto*, por ser la metodología idónea para analizar medidas que inciden en el derecho a la intimidad y la protección de datos sensibles¹².

Dicho lo anterior, desde mi perspectiva la obtención de datos biométricos persigue **una finalidad constitucionalmente imperiosa**: tutelar la seguridad pública, que de acuerdo con el artículo 21 de la Constitución General es una función del Estado encaminada a salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas. Así se desprende del propio texto de la ley, la cual dispone que el único fin del padrón es “colaborar con las autoridades competentes en materia de seguridad y justicia en asuntos relacionados con la comisión de delitos”¹³. Por otra parte, del procedimiento legislativo se desprende que la reforma responde al crecimiento exponencial de delitos cometidos a través de dispositivos móviles, como el secuestro y la extorsión¹⁴.

En cambio, la medida **no está estrechamente vinculada** con la finalidad constitucionalmente imperiosa que persigue. El acceso a los datos biométricos de la persona que se encuentra registrada como titular de una línea telefónica es insuficiente para vincularla con la comisión de un delito relacionado con la misma. En todo caso, sirve para evidenciar quién la contrató, pero es inverosímil que una llamada de extorsión se realice desde un número telefónico asociado a la persona que la hace, pues las extorsiones nunca se realizan a partir de los teléfonos que tiene a su nombre el extorsionador.

Incluso, el régimen transitorio reconoce este problema al establecer que se realizarán campañas para incentivar la denuncia de robo o pérdida de equipos celulares y prevenir el robo de identidad¹⁵. Es decir, el sistema pretende convertir obligaciones estatales de persecución de delitos en responsabilidades individuales.

De igual modo, no puede ignorarse que en la exposición de motivos del Decreto por el que se eliminó el antiguo Registro Nacional de Usuarios de Telefonía Móvil, mejor conocido como RENAUT, se argumentó que éste no había tenido frutos en la prevención, investigación y persecución de los delitos como el secuestro y la extorsión. Asimismo, se consideró la opinión de especialistas que afirmaban que la obligación de registrar teléfonos móviles generaba incentivos para el robo de estos dispositivos¹⁶.

Por estas razones, considero que la fracción VI del artículo 180 ter de la Ley Federal de Telecomunicaciones y Radiodifusión es inconstitucional no sólo por pertenecer a un sistema normativo inválido, sino también lo sería por los vicios concretos que señalo en relación con este precepto en lo individual.

b) Los requisitos para el acceso a los datos del PANAUT.

El artículo 180 septimus de la Ley Federal de Telecomunicaciones y Radiodifusión¹⁷ dispone que las autoridades de seguridad de procuración y administración de justicia podrán acceder a la información del PANAUT, siempre que cuenten con la facultad expresa para requerir al Instituto los datos del padrón.

¹² Esta ha sido mi postura desde la AI 21/2013 de mi ponencia en la que se analizó la constitucionalidad del artículo 275 Bis del Código de Procedimientos Penales del Estado de Nuevo León que establecía la obligación de los testigos de acreditar su identidad con una prueba de ácido desoxirribonucleico (ADN), página 75 de la sentencia.

¹³ **Ley Federal de Telecomunicaciones y Radiodifusión.**

Artículo 180 Bis. El Instituto expedirá las disposiciones administrativas de carácter general para la debida operación del Padrón Nacional de Usuarios de Telefonía Móvil, el cual es una base de datos con información de las personas físicas o morales titulares de cada línea telefónica móvil que cuenten con número del Plan Técnico Fundamental de Numeración y **cuyo único fin 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.**

¹⁴ Exposición de motivos de la Iniciativa que adiciona el artículo 15 de la Ley Federal de Telecomunicaciones y Radiodifusión, a cargo del diputado Manuel Gómez Ventura, del grupo parlamentario de Morena, página 1.

¹⁵ **Sexto.** El Gobierno Federal, a través de la Secretaría de Comunicaciones y Transportes, la Secretaría de Seguridad y Protección Ciudadana y el Instituto Federal de Telecomunicaciones, así como los concesionarios de telecomunicaciones, deberán realizar campañas y programas informativos a sus clientes o usuarios para incentivar la obligación 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.

¹⁶ INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN, ADICIONAN Y DEROGAN DIVERSAS DISPOSICIONES DEL CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES, DEL CÓDIGO PENAL FEDERAL, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y DE LA LEY QUE ESTABLECE LAS NORMAS MÍNIMAS SOBRE READAPTACIÓN SOCIAL DE SENTENCIADO, consultado en <https://legislacion.scjn.gob.mx/Buscador/Paginas/wfProcesoLegislativoCompleto.aspx?q=Fahf/ZCcCGTRH7BTx0eHtKCK2XcouBu2Gk48zkHs/UVDTxCqJtJ8Oy7bbYPGtKQvprSxMyIppT7Yrvuvbdkaxg==>.

¹⁷ **Ley Federal de Telecomunicaciones y Radiodifusión.**

Artículo 180 Septimus. [...]

Las autoridades de seguridad de procuración y administración de justicia, que conforme a las atribuciones previstas en sus leyes aplicables cuenten con la facultad expresa para requerir al Instituto los datos del Padrón Nacional de Usuarios de Telefonía Móvil, podrán acceder a la información correspondiente de acuerdo con lo establecido en los artículos 189 y 190 de esta Ley y demás disposiciones relativas.

Al respecto, me parece que, a la luz del derecho a la vida privada, reconocido en los artículos 16 de la Constitución General y 11 de la Convención Americana sobre Derechos Humanos¹⁸, esta disposición resulta inconstitucional porque al no requerir orden judicial previa para acceder a la información contenida en el PANAUT, se actualiza una injerencia arbitraria en la privacidad de las personas. Es decir, en el haz de facultades positivas que reconoce la Constitución a fin de que éstas puedan controlar y decidir sobre su información personal¹⁹.

Así, de manera reiterada he sostenido una interpretación sistemática y evolutiva del artículo 16 constitucional, en el sentido de que se requiere control judicial previo *en aquellos casos en que puedan vulnerarse de igual o mayor manera los “intereses de privacidad” tutelados en dicha norma*. Es decir, he sostenido una interpretación no limitada a los supuestos que dicho artículo prevé de forma expresa, como las órdenes de cateo para acceder a un domicilio, la intervención de comunicaciones privadas y las medidas que afectan la libertad personal como la orden de aprehensión y de arraigo²⁰.

Con base en dicha interpretación, he votado por la inconstitucionalidad de normas que permiten a las autoridades acceder a bases de datos relacionadas con derechos patrimoniales, entre otras²¹.

En el presente caso, el párrafo tercero del artículo 180 septimus permite a autoridades *“de seguridad de procuración y administración de justicia”* acceder a cualquier tipo de información contenida en el PANAUT, lo que entraña una vulneración a la privacidad de igual o mayor importancia a los casos expresamente previstos en el artículo 16 constitucional, pues las tecnologías biométricas trabajan sobre las características físicas, fisiológicas o conductuales de una persona, permitiendo identificarla. Esto no es menor, porque modifica la relación entre cuerpo e identidad: transforma el cuerpo humano en datos legibles por máquinas. Así, considero que es inconstitucional por no requerir orden judicial previa para el acceso al padrón.

Por último, no desconozco que existen casos en que este control puede admitir excepciones, como cuando existe urgencia o puede ponerse en riesgo la vida o la integridad de una persona²², pero la norma antes mencionada no acota a estos supuestos su ámbito de aplicación ni tampoco puede llegarse al extremo de que las autoridades puedan tener este tipo de datos, sin orden judicial.

En esas condiciones, sostengo que el párrafo tercero del artículo 180 septimus de la Ley Federal de Telecomunicaciones y Radiodifusión es inconstitucional por razones adicionales a aquellas que justifican la invalidez del sistema.

Consecuentemente, aun cuando comparto la invalidez de todo el sistema que regula y crea el PANAUT, lo cierto es que las razones antes expuestas constituyen aspectos adicionales que reafirman la inconstitucionalidad del Decreto impugnado.

Ministro Presidente, **Arturo Zaldívar Lelo de Larrea**.- Firmado electrónicamente.- Secretario General de Acuerdos, Lic. **Rafael Coello Cetina**.- Firmado electrónicamente.

EL LICENCIADO **RAFAEL COELLO CETINA**, SECRETARIO GENERAL DE ACUERDOS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN: CERTIFICA: Que la presente copia fotostática constante de siete fojas útiles, concuerda fiel y exactamente con el original firmado electrónicamente del voto concurrente formulado por el señor Ministro Presidente Arturo Zaldívar Lelo de Larrea, en relación con la sentencia del veintiséis de abril de dos mil veintidós, dictada por el Pleno de la Suprema Corte de Justicia de la Nación en 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 y diversos Senadores Integrantes de la LXIV Legislatura. Se certifica con la finalidad de que se publique en el Diario Oficial de la Federación.- Ciudad de México, a siete de noviembre de dos mil veintidós.- Rúbrica.

¹⁸ **Convención Americana sobre Derechos Humanos.**

Artículo 11. Protección de la Honra y de la Dignidad.

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

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

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

¹⁹ En la acción de inconstitucionalidad 100/2019 formulé un voto concurrente en el que me pronuncié sobre la constitucionalidad del artículo 190 de la Ley Nacional de Extinción de Dominio, que permitía acceder a bases de datos necesarias para la procedencia de la acción, involucradas con la operación, registro y control de derechos patrimoniales. Ello, en tanto la mayoría consideró que constituía una restricción desproporcional al derecho a la protección de datos personales. En cambio, yo me decanté por analizar la norma a la luz del derecho a la privacidad en los términos que propongo en este voto.

²⁰ Ídem.

Del mismo modo que en el voto relativo a la acción de inconstitucionalidad 10/2014 y su acumulada 11/2014 resueltas el veintidós de marzo de dos mil dieciocho y en el amparo directo en revisión 502/2017 resuelto en sesión del veintidós de noviembre de dos mil diecisiete.

²¹ Ídem.

²² Como establecí en el voto concurrente de la acción de inconstitucionalidad 32/2012.