VOTO CONCURRENTE 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 grada 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 Interamericano[1], relativos a la Confidencialidad y Seguridad de los Datos, incorporados en los artículos 31 a 42 de la Ley General de 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 General[2].

II. Consideraciones adicionales de inconstitucionalidad del Decreto por el que se crea y regula el PANAUT.

---

[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.

[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.

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 toral 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 torales 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 Radiodifusión[3] establece la obligación a los usuarios de telefonía móvil de otorgar sus datos biométricos[4] 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

---

[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.

acceso a la información y los derechos de asociación e igualdad[5], dada la relación indisoluble entre ellos[6].

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 sociales[7], 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.

---

[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.

[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 29° 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&lID=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.

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 legítimo[8].

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 Datos[9], como el Convenio para la Protección de las

---

[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, parras. 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

Personas con respecto al Tratamiento de Datos Personales[10] 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 Obligados[11].

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 sensibles[12].

---

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…

[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.

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 extorsión[14].

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

---

[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.

robo o pérdida de equipos celulares y prevenir el robo de identidad[15]. 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 dispositivos[16].

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 Radiodifusión[17] dispone que las autoridades de seguridad de

---

[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. […]

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.

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 Humanos[18], 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 personal[19].

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

---

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.

[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.

de comunicaciones privadas y las medidas que afectan la libertad personal como la orden de aprehensión y de arraigo[20].

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 otras[21].

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 persona[22], 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.

---

[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.

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