PROPOSICIÓN CON PUNTO DE ACUERDO, POR EL QUE SE EXHORTA AL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI) Y AL INSTITUTO FEDERAL DE TELECOMUNICACIONES (IFT), A REVISAR LOS PROCEDIMIENTOS DEL AVISO DE PRIVACIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES SENSIBLES POR PARTE DE LAS EMPRESAS QUE OTORGAN SERVICIOS DE TELEFONÍA MÓVIL

Paulina Rubio Fernández y María Elena Pérez-Jaén Zermeño, diputadas federales, integrantes de la LXV Legislatura de la Cámara de Diputados del honorable Congreso de la Unión, e integrantes del Grupo Parlamentario del Partido Acción Nacional, con fundamento en los artículos 58, 59 y 60 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, presentamos la siguiente proposición con Punto de Acuerdo, con base en las siguientes:

Consideraciones

El artículo 3 fracción VI de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFDPPP), define datos personales sensibles, como 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.

El artículo 9 de la misma Ley señala que, tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

Esto es, el tratamiento de datos sensibles conlleva la realización de una serie de garantías a favor de sus titulares, como la obtención de su consentimiento expreso y por escrito.

Como se puede advertir, en la LFDPPP no existe una referencia expresa para considerar los datos biométricos como sensibles, lo que no obsta para que así se les considere en la

implementación y aplicación de la LFDPPP, ya que al aludir en su redacción a datos personales sensibles como aquellos datos personales que afecten a la esfera más íntima de su titular, aquellos cuya utilización indebida pueda dar origen a discriminación o que conlleven un riesgo grave para éste, permite que, a partir de esa fórmula genérica, se incluyan los datos biométricos.

En cuanto a la consideración que se ha hecho respecto de los datos biométricos en México, y en el derecho comparado, en su carácter de dato sensible, existen diversas referencias que conviene mencionar.

En la legislación de datos personales para el ámbito público, del orden estatal, es posible encontrar referencias expresas a los datos biométricos como datos sensibles en los casos de Campeche, Chiapas, Chihuahua, Ciudad de México, Guanajuato, Guerrero, Hidalgo, Jalisco, Nuevo León, Puebla, Quintana Roo, San Luis Potosí, Sonora, Tamaulipas y Zacatecas.

El hecho de que 15 leyes locales de datos personales refieran a los datos biométricos, como sensibles, resulta relevante desde tres ópticas:

1. Que ha sido explorado y determinado el hecho de considerar los datos biométricos con el carácter de sensibles, debido a sus implicaciones en la vida de las personas;
2. Que el derecho a la protección de datos personales, en su carácter de derecho fundamental, debería regirse por el principio de indivisibilidad, previsto en el artículo 1o constitucional, por lo que debería ser garantizado por igual en todos los ámbitos de gobierno y de los particulares, ya que de otro modo la fragmentación podría provocar la existencia de titulares con mejor o menor protección de sus datos según la ley que les aplique y su forma de implementación, y
3. Que si bien de la definición general de datos sensibles es posible y válido interpretar que los datos biométricos forman parte de esa categoría, lo cierto es que se está en presencia de un tema que bien podría ser incluido en la lista de ejemplos enunciativos de la legislación de datos personales, para no dejar lugar a dudas, en atención a las implicaciones de su tratamiento en la esfera de derechos de sus titulares.

El 16 de abril de 2021 se publicó el Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, en el Diario Oficial de la Federación, el cual habilitó la posibilidad de que las empresas telefónicas recabaran datos biométricos.

El 25 de abril de 2022 la Suprema Corte de Justicia de la Nación (SCJN) declaró su inconstitucionalidad[1] (acción de inconstitucionalidad 82/2021 y su acumulada 86/2021).

El propio Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en su demanda de acción de inconstitucionalidad, contra 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 (DOF) el dieciséis de abril de dos mil veintiuno, en sus páginas 24 y 25 señaló lo siguiente:

> [...]
>
> Pero no sólo se viola el derecho de protección a los datos personales y la privacidad sino que se viola la intimidad de los ciudadanos, ya que dentro de los datos personales existe una categoría que precisamente afecta los aspectos más íntimos16 de las personas, y que se denominan datos personales sensibles, entre los que podemos encontrar los datos biométricos, toda vez que se encuentran dirigidos a identificar de manera unívoca a las personas, además de que pueden dar cuenta del origen racial o étnico, entre otras características. Por lo que, si los datos personales sensibles, como los datos biométricos, se encuentran protegidos por el derecho a la intimidad, vulnerar la protección a estos datos implicará vulnerar un derecho personalísimo -la intimidad- que protege el contenido más profundo de la privacidad y que debe estar radicalmente vedado.
>
> [...]

También, la SCJN determinó[2], en la resolución a la acción de inconstitucionalidad 82/2021

---

[1] Véase en: https://www.scjn.gob.mx/sites/default/files/actas-sesiones-publicas/documento/2022-05-09/42%20-%2025%20de%20abril%20de%202022.pdf Consultado el 2 de junio de 2022.

[2] SCJN. Consultable en el acta de la sesión pública número 42, ordinaria, del veinticinco de abril de dos mil veintidós. Véase en: https://www.scjn.gob.mx/sites/default/files/actas-sesiones-publicas/documento/2022-05-09/42%20-%2025%20de%20abril%20de%202022.pdf Consultado el 3 de junio de 2022.

y su acumulada 86/2021, que los datos biométricos son datos sensibles, para mejor referencia se cita el texto correspondiente:

> [...] así como lo determinado en los precedentes de la Primera Sala, por lo que, al imponerse a los usuarios de telefonía móvil la obligación de entregar su información privada, íntima y datos personales, incluyendo datos sensibles, así como la correlativa facultad de terceros particulares y al Estado para recopilarlos y acceder a ellos, se impacta la referida autodeterminación informativa, ya que esta entrega no es optativa a fin de adquirir o conservar este servicio, además de que el usuario no define el uso y destino que se le dará a su información —su consentimiento— y, por tanto, la afectación a estos derechos humanos es intenso en función de cuatro elementos que se destacan de este sistema normativo: 1) la información que se ordena recabar se relaciona con los aspectos más íntimos de la persona, como sus datos biométricos y demás información que, en su conjunto, permite extraer conclusiones muy precisas sobre la esfera de su privacidad [...]

Ese reconocimiento que hacen las leyes locales, la SCJN y el INAI, respecto de los datos sensibles se encuentra en armonía con lo que el derecho comparado prevé, específicamente, el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), que en su artículo 9, relativo al tratamiento de categorías especiales de datos, el equivalente a nuestro régimen de datos sensibles, considera los datos biométricos, expresamente, como parte de los datos que ameritan una protección particular y reforzada.

Por lo que refiere al Comité Europeo de Protección de Datos Personales, en su carácter de supervisor y garante del RGPD, existen pronunciamientos claros en torno al tratamiento de los datos biométricos, por ejemplo, en las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, al tenor de lo siguiente[3]:

> [...]
>
> 5.1 Consideraciones generales para el tratamiento de datos biométricos

[3] Véase en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_es.pdf Consultado el 02 de junio de 2022.

73. El uso de datos biométricos y, en particular, del reconocimiento facial conllevan elevados riesgos para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando debidamente los principios de licitud, necesidad, proporcionalidad y minimización de datos tal y como establece el RGPD. Aunque la utilización de estas tecnologías se pueda percibir como particularmente eficaz, los responsables del tratamiento deben en primer lugar evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos de lograr su fin legítimo del tratamiento.

[...]

86. Por último, cuando el artículo 9 del RGPD exige el consentimiento, el responsable del tratamiento no puede supeditar el acceso a sus servicios a la aceptación del tratamiento biométrico. En otras palabras, y especialmente cuando el tratamiento biométrico se utiliza con fines de autenticación, el responsable del tratamiento debe ofrecer una solución alternativa que no implique el tratamiento biométrico, sin restricciones ni coste adicional para el interesado. Esta solución alternativa también se necesita para las personas que no cumplen las limitaciones del dispositivo biométrico (imposibilidad de registro o lectura de los datos biométricos, situación de incapacidad que dificulta el uso, etc.) y como anticipación a la falta de disponibilidad del dispositivo biométrico (como una avería del dispositivo), se debe instalar una «solución de copia de seguridad» para garantizar la continuidad del servicio prestado, limitado no obstante al uso excepcional.

[...]

En ese sentido, en el tratamiento de datos biométricos se debería partir de dos premisas fundamentales, al menos, a saber:

1. Debería limitarse a los casos plenamente justificados, teniendo particular cuidado con los principios de licitud, proporcionalidad y minimización, para efectos de verificar esa justificación, principios previstos en la LFDPPP y su Reglamento;
2. Resulta fundamental que, todo responsable que decida tratar datos biométricos, desarrolle, previo a su implementación, una evaluación integral en la que se analice el impacto que dicho tratamiento puede traer a los derechos y libertades

fundamentales de los titulares, de modo que sea posible demostrar que no existen medios menos intrusivos para alcanzar la finalidad legítima perseguida. Al respecto, la LFDPPP prevé en su artículo 38, entre las atribuciones del INAI, la elaboración de estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes.

También, en el ámbito americano de los derechos humanos, específicamente en los principios[4] actualizados del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales, con anotaciones, en la definición de datos sensibles, establecen lo siguiente:

[...]

Datos Personales Sensibles. El término "Datos Personales Sensibles" se refiere a una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas. 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. En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria.

[...]

El hecho de que los datos biométricos resulten altamente eficaces para cumplir con determinados objetivos, como la identificación de las personas, no justifica, por sí misma, la necesidad de su tratamiento, en realidad, en el ámbito de los datos personales, el tratamiento de los datos biométricos para lograr la identificación unívoca de su titular les confiere la consideración de datos especialmente protegidos o sensibles. Esa alta eficacia

[4] Véase en: https://www.redipd.org/sites/default/files/2021-05/CJI-doc 638-21.pdf Consultado el 02 de junio de 2022.

de los datos biométricos puede representar, en contrapartida un alto riesgo para sus titulares, de desviarse las finalidades para los que se obtuvieron, por citar un ejemplo.

De acuerdo con las consideraciones descritas, con o sin referencia expresa en la legislación en materia de datos personales, existe claridad, tanto en México como en el derecho comparado, sobre la calidad de dato sensible de los datos biométricos, en general, así como sobre la necesidad de desarrollar evaluaciones de impacto para determinar la pertinencia de su tratamiento a la luz de los principios y deberes que rigen el tratamiento de los datos personales.

Conforme a lo previsto en el artículo 38 de la LFDPPP el INAI posee atribuciones para vigilar y verificar su cumplimiento, interpretarla, proporcionar apoyo técnico a los responsables y para emitir criterios y recomendaciones, entre otras.

Otro de los aspectos fundamentales en el tratamiento de datos biométricos se encuentra en el aviso de privacidad, que es un documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales. El aviso de privacidad deberá contener, al menos, la siguiente información:

I. La identidad y domicilio del responsable que los recaba;

II. Las finalidades del tratamiento de datos;

III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;

IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en la Ley;

V. En su caso, las transferencias de datos que se efectúen, y

VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en la Ley.

El Artículo 8 de la LFDPPP, estipula que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, y se entiende que el titular consiente tácitamente el

tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

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.

El artículo 17 de la Ley multicitada, señala que el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

I. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y

II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos su finalidad y las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Al respecto, los Lineamientos del Aviso de Privacidad, en su numeral tercero, definen la puesta a disposición el aviso de privacidad de forma personal como el acto en el cual el responsable hace del conocimiento del titular el aviso de privacidad, con la presencia física de ambos. Esto es, en los casos en los que la interacción entre responsable y titular se produzca de forma presencial, el responsable debe entregar o hacer del conocimiento del titular el aviso de privacidad, en ese momento, durante la citada interacción entre ambos.

Como ha quedado señalado, uno de los principios esenciales en el tratamiento de datos

personales sensibles, como son los datos biométricos, es el principio de licitud conforme al cual los datos personales deben recabarse y tratarse de manera lícita conforme a las disposiciones establecidas en la normatividad aplicable.

Al respecto, resulta ineludible la determinación de la SCJN, del 25 de abril de 2022, sobre la invalidez de la totalidad del sistema normativo que integra el Decreto de reformas a la Ley Federal de Telecomunicaciones y Radiodifusión de abril de 2021, para crear un Padrón Nacional de Usuarios de Telefonía Móvil (Panaut).

El caso es que, el Aviso de Privacidad de Telcel[5], y convendría verificar el caso de otras compañías de telefonía celular al respecto, establece lo siguiente:

> ***Datos personales sensibles***
>
> *Telcel podrá dar tratamiento a datos biométricos referentes a sus huellas dactilares con la finalidad de identificarle y acreditar su identidad para la provisión de los Servicios y futuras operaciones que usted realice ante Telcel.*
>
> ***Fuentes indirectas de obtención de datos personales.***
>
> *En aquellos casos en los que Telcel cuente con una base de legitimación, podrá obtener información vinculada a usted a través de las siguientes fuentes: (i) comunicaciones de datos personales por parte de empresas afiliadas (Para efectos del presente Aviso de Privacidad, afiliada significa respecto de una empresa determinada cualquier otra empresa que, directa o indirectamente, a través de uno o más intermediarios tiene el control, es controlada o se encuentra bajo el control común de la empresa especificada), subsidiarias y/ o entidades controladoras de Telcel ("Empresas del Grupo"); (ii) cuando terceros con los que Telcel tenga celebrados acuerdos comerciales le proporcionen información relacionada con usted, incluyendo sociedades de información crediticia; y (iii) cuando la información provenga de fuentes de acceso público.*
>
> *Finalidades primarias del tratamiento.*
>
> *Telcel tratará los datos personales descritos en el presente Aviso para llevar a cabo alguna o todas las actividades necesarias para el desarrollo y cumplimiento de las obligaciones que se originen y deriven de los Servicios que incluyen las siguientes finalidades:*
>
> *(...)*
>
> *Elaborar análisis y estudios relacionados con su comportamiento de consumos, así como investigaciones y monitoreo periódicos sobre su comportamiento*

[5] Véase: https://www.telcel.com/aviso-de-privacidad Consultado el 21 de mayo de 2022.

crediticio, incluyendo proporcionar información a las sociedades de información crediticia correspondientes.

Finalidades secundarias del tratamiento.

Telcel tratará sus datos personales para llevar a cabo alguna o todas las finalidades secundarias que se mencionan a continuación:

- *Informarle del lanzamiento o cambios de nuevos productos, bienes, servicios, promociones y/u ofertas de Telcel de acuerdo con sus intereses, así como de otras Empresas del Grupo y/o socios comerciales incluyendo llamadas telefónicas el envío de comunicaciones a través de correos electrónicos, mensajes cortos y demás medios de comunicación físicos y/o electrónicos;*

- *Realizar tratamientos de técnicas de análisis masivo de datos para actividades de perfilamiento a partir de combinar información facilitada por usted, la obtenida de fuentes de acceso público, incluyendo redes sociales, y aquella información que se pueda inferir u obtener como resultado de la aplicación de diversas tecnologías de análisis de datos. Lo anterior para contactarle y enviarle información de carácter publicitario, promocional y/o informativo que consideramos puede resultar de su interés;*

- *Generar perfiles y hábitos de consumo para que nuestros socios comerciales puedan contactarle y enviarle información de carácter publicitario, promocional y/o informativo que consideren de su interés y/o para que puedan valorar, conforme a sus procedimientos internos, si usted es susceptible de obtener el servicio que hubiere solicitado ante dicho tercero;*

Si usted no desea que Telcel trate sus datos personales para alguna de las finalidades descritas en este apartado, por favor envíe un correo electrónico a datospersonales@telcel.com. Usted podrá cambiar de opción en cualquier momento.

Es importante que tenga presente que, en caso de otorgar su consentimiento, este seguirá siendo válido incluso cuando hubiere terminado la relación jurídica entre usted y Telcel, lo que significa que Telcel podrá seguir tratando sus datos personales necesarios para cumplir con las presentes finalidades secundarias.

Necesario obtener su consentimiento

Si usted no se opone, Telcel podrá transferir sus datos personales a socios comerciales y/o terceros, incluyendo instituciones bancarias para que estas puedan contactarle y ofrecerle bienes y/o servicios que resulten de su interés, o bien, para que puedan determinar si usted es sujeto a adquirir los bienes y/o servicios que dichos socios comerciales y/o terceros ofrecen.

Si usted no desea que Telcel lleve a cabo la transferencia de referencia, por favor envíe un correo electrónico a datospersonales@telcel.com Usted podrá cambiar

de opción en cualquier momento.

Sin embargo, cuando un usuario contrata o renueva su contrato con la compañía telefónica, se otorgan documentos que se deben firmar, como el contrato de adhesión, y se incluye una aceptación total del aviso de privacidad, más no el aviso propiamente, sino un sitio web en donde se puede consultar. En ese sentido, el mecanismo en que se pone a disposición del usuario el aviso de privacidad con la información del tratamiento que la compañía pretende dar a los datos personales, incluidos datos sensibles como los datos biométricos, genera muy serias dudas, por lo que refiere al cumplimiento del principio de información, en tanto que no se hace la entrega o del conocimiento del titular el aviso de privacidad, en ese momento, durante la interacción entre la telefónica y el cliente.

Podría ser una violación a lo dispuesto en el art. 17 de la LFDPPP, pues no se recaba el dato de forma clara y fehaciente, y en oposición se da una aceptación engañosa, y, cuando menos, poco informada por parte del usuario, titular del derecho probablemente violentado, con lo que, a su vez, se estaría contraviniendo el principio de lealtad previsto en el artículo 7 de la LFDPPP y 44 del Reglamento de la LFDPPP.

Otra consideración de alta relevancia respecto del tratamiento de datos personales que lleva a cabo Telcel está en una de sus finalidades primarias, descrita en su aviso de privacidad, al tenor de lo siguiente:

> [...]
>
> **Finalidades primarias del tratamiento**
>
> Telcel tratará los datos personales descritos en el presente Aviso para llevar a cabo alguna o todas las actividades necesarias para el desarrollo y cumplimiento de las obligaciones que se originen y deriven de los Servicios que incluyen las siguientes finalidades:
>
> - Acreditar y verificar su identidad conforme a nuestros procedimientos y políticas, incluyendo la verificación de los datos de su Credencial para Votar y similitud de huellas dactilares ante el Instituto Nacional Electoral.
>
> [...]

Se trata de un aspecto fundamental en el ámbito del consentimiento previo del titular de los datos personales, ya que el propio Instituto Nacional Electoral así lo establece desde el aviso de privacidad integral del Padrón Electoral[6], como una condición indispensable de parte de cualquier institución pública o privada, para poder utilizar el servicio de verificación, para mejor referencia, se hace la cita del apartado correspondiente:

> [...]
>
> ¿Para qué finalidad o finalidades utilizamos tus datos personales?
>
> Los datos personales que la ciudadanía proporciona al Instituto, así como los que genera éste a partir de la información recabada de la ciudadanía, son estrictamente confidenciales y serán tratados para:
>
> [...]
>
> El nombre completo, huellas dactilares y clave de elector, previo consentimiento de sus titulares ante las instituciones públicas y/o privadas, podrán utilizarse para el Servicio de Verificación de Datos de la Credencial para Votar, con la finalidad de corroborar que la Credencial para Votar que se presenta para trámites o servicios sea auténtica, a fin de proteger su identidad y evitar usurpación o robo de dicha identidad y con ello, la posible comisión de un ilícito por parte de terceros.
>
> [...]

Conforme a lo anterior, debería haber claridad total sobre la necesidad de recabar el consentimiento y de que ese consentimiento sea expreso y por escrito, al ser los datos biométricos datos sensibles.

En consecuencia, consideramos que tanto el INAI, como el Instituto Federal de Telecomunicaciones (IFT), en el ámbito de sus respectivas competencias, deben investigar, revisar y, en su caso actuar de conformidad a derecho con esta probable irregularidad.

---

[6] Véase: https://portal.ine.mx/wp-content/uploads/2022/04/DERFE-AvisPrivacidadIntegral-PadronElectoral.pdf Consultado el 02 de junio de 2022.

El INAI, en términos del Artículo 38 de la LFDPPP, tiene por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados.

Como ya ha quedado señalado, el derecho a la protección de datos personales en México, es universal, por lo que se considera conveniente que también se hagan extensivas estas consideraciones sobre datos biométricos para el tratamiento de datos en el ámbito público, en donde si bien es cierto existen diversas leyes que consideran los datos biométricos como datos sensibles, también lo es que no todas las leyes estatales poseen esa consideración sobre los datos biométricos, por lo que también resultaría valiosa la colaboración del el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para promover, entre todas las entidades federativas y la Ciudad de México, estándares que fortalezcan el principio constitucional de indivisibilidad de este derecho, en su espacio de competencias, conforme a lo establecido en los artículos 10, 11, 12, 13, 14 y 15 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tanto que el IFT, en términos del artículo 7 de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), tiene a su cargo la prestación de los servicios de radiodifusión y de telecomunicaciones, así como del acceso a la infraestructura activa y pasiva y otros insumos esenciales, sin perjuicio de las atribuciones que corresponden a otras autoridades en los términos de la legislación correspondiente.

Por su parte, en el artículo 15, fracción XXVII de la LFTR se establece entre las atribuciones del IFT la de vigilar el cumplimiento a lo dispuesto en los títulos de concesión otorgados en materia de telecomunicaciones y radiodifusión y ejercer facultades de supervisión y verificación, a fin de garantizar que la prestación de los servicios se realice con apego a esta Ley y a las disposiciones legales, reglamentarias y administrativas aplicables, a los títulos de concesión y a las resoluciones expedidas por el propio IFT.

Por su parte, en el artículo 190 de la LFTR, en el contexto de las obligaciones en materia de seguridad y justicia se establece que los concesionarios de telecomunicaciones y, en su caso, los autorizados deben observar lo dispuesto en la LFDPPP, en el tratamiento de

datos personales que lleven a cabo. Es decir, no existen dudas de que los concesionarios de telecomunicaciones y, en su caso, los autorizados deben observar lo dispuesto en la LFDPPP pero incluso en el caso de las obligaciones en materia de seguridad y justicia, que contienen algunas excepciones en materia da datos, se reafirma la necesidad de que los citados concesionarios y autorizados cumplan con la LFDPPP.

En ese sentido, las facultades de vigilancia de parte del IFT también pasan por esta temática, no para efectos de aplicar algún tipo de sanción conforme a lo establecido en la LFDPPP, ya que eso le corresponde al INAI, sino para aplicar las medidas administrativas a que haya lugar en torno al impacto que este tipo de situaciones provoca en la prestación de servicios a cargo de los concesionarios y autorizados.

Por lo anteriormente expuesto esta Comisión Permanente del H. Congreso de la Unión, extiende el siguiente Punto de Acuerdo:

PRIMERO. La Comisión Permanente del Honorable Congreso de la Unión de la LXV Legislatura exhorta, respetuosamente, al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), para que en el ámbito de sus competencias, vigile y verifique el cumplimiento de los principios de licitud, lealtad, consentimiento, proporcionalidad, información y responsabilidad en el tratamiento de datos biométricos para "...Acreditar y verificar su identidad conforme a nuestros procedimientos y políticas, incluyendo la verificación de los datos de su Credencial para Votar y similitud de huellas dactilares ante el Instituto Nacional Electoral...", por parte de las empresas de Telefonía Móvil. En el caso de advertir la existencia de infracciones, proceda a la determinación y aplicación de las sanciones correspondientes, conforme a derecho.

SEGUNDO. La Comisión Permanente del Honorable Congreso de la Unión de la LXV Legislatura exhorta, respetuosamente, al Instituto Federal de Telecomunicaciones (IFT) para que en el ámbito de sus competencias, investigue y, en su caso, proceda, ante la posible vulneración, por parte de las empresas de Telefonía Móvil, sobre el cumplimiento a lo dispuesto en los títulos de concesión otorgados en materia de telecomunicaciones y radiodifusión que garantice la prestación de los servicios se realice con apego a la Ley y a las disposiciones legales, reglamentarias y administrativas aplicables, en específico, sobre el procedimiento para dar a conocer a sus usuarios el Aviso de Privacidad, mediante el

cuál estipulan el tratamiento que le dará a sus datos personales, particularmente de los datos personales sensibles, como los de índole biométrico, el cual debe ser de forma clara y fehaciente, para aplicar las medidas administrativas a que haya lugar en torno al impacto que este tipo de situaciones provoca en la prestación de servicios a cargo de los concesionarios y autorizados.

TERCERO. La Comisión Permanente del Honorable Congreso de la Unión de la LXV Legislatura, exhorta respetuosamente a los integrantes del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para promover entre todas las entidades federativas y la Ciudad de México estándares y prácticas que fortalezcan el principio constitucional de indivisibilidad de este derecho, en el ámbito de su competencia.

Paulina Rubio Fernández

Diputada Federal

María Elena Pérez-Jaén Zermeño

Diputada Federal

Cámara de Senadores, en la Ciudad de México a 15 de junio de 2022