

SEGUNDA PARTE

I. ¿QUÉ ES EL INAI?

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es un organismo constitucional autónomo, garante del cumplimiento de dos derechos fundamentales: el acceso a la información pública y el derecho de protección de datos personales.

El INAI garantiza que los órganos autónomos, partidos políticos, fideicomisos, fondos públicos, sindicatos, así como cualquier autoridad en el ámbito federal o persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad entregue la información pública que se solicite. Además, respalda el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona tiene con respecto a su información.

La Ley Federal de Transparencia y Acceso a la Información Pública obliga a los poderes Ejecutivo, Legislativo y Judicial, así como a los organismos constitucionales autónomos, a tener control sobre dicha información. Así, el INAI tiene facultades para vigilar su cumplimiento y resolver sobre negativas de acceso a la información, únicamente respecto a las dependencias y entidades de la administración pública federal.

1. Principios del derecho de acceso a la información

- El derecho de acceso a la información es un derecho fundamental de toda persona.

- El derecho de acceso a la información se aplica a todas las entidades públicas, a todos los poderes del Estado y a todas aquellas entidades privadas que realicen funciones públicas.
- Se aplica a toda la información elaborada, recibida o en posesión de las entidades públicas, sin importar cómo esté almacenada.
- Realizar solicitudes debe ser de una manera sencilla, rápida y gratuita.
- Los funcionarios tienen la obligación de ayudar a los solicitantes.
- El principio de publicidad de la información, el secreto y la denegación de la información son la excepción.
- Las denegaciones de acceso a la información deben ser limitadas y estar debidamente motivadas.
- Toda persona tiene el derecho a recurrir las denegaciones de acceso o la no contestación a las solicitudes realizadas.
- Las entidades públicas, a iniciativa propia, deben poner a disposición del público la información básica y esencial sin que sea necesario realizar una solicitud.
- El derecho de acceso a la información debe ser garantizado por un órgano independiente.

2. *Inscripción en el Sistema de Personas*

El Sistema de Personas es una aplicación informática desarrollada por el INAI con el objetivo de mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades.

En el Sistema de Personas se registra e informa sobre las transmisiones, modificaciones y cancelaciones de los sistemas de datos personales, así como la información general de éstos:

- Nombre de la base de datos personales.
- La unidad administrativa en la que se encuentra.
- Nombre, cargo, teléfono y correo electrónico del responsable.

- La finalidad de la base de datos.
- La normatividad aplicable.²⁷

3. Ejemplos de casos a debate en el INAI

Caso	Descripción
Estado de salud del presidente de la República	El INAI determinó que no se cumplía con el principio de razonabilidad para determinar que el estado de salud del titular del Ejecutivo Federal debía considerarse como información pública. El presidente de la República es una figura pública, pero su salud se considera un dato personal.
Los expedientes médicos en instituciones de salud públicas	El INAI decretó que el paciente debe tener acceso a su expediente médico, pues es el titular de la información relativa a su estado de salud.
Las fotografías de servidores públicos	El criterio adoptado por el INAI fue considerar la fotografía de servidores públicos como un dato personal, pues nada hace más identificable a una persona que su imagen, aunado al hecho de que no se contribuye a la transparencia gubernamental o a la rendición de cuentas al publicar dicha información.

Fuente: Edgardo Martínez Rojas, *El derecho a la protección de datos personales en la Administración Pública Federal*.

²⁷ Cfr. Edgardo Martínez Rojas, *op. cit.*

No obstante, el análisis del INAI ha considerado algunas excepciones:

<i>Caso</i>	<i>Descripción</i>
Estados de cuenta bancarios de servidores públicos	El INAI estableció que se trata de datos personales, pues es información relativa a su patrimonio, a menos que se trate de información relativa a una cuenta corporativa integrada con recursos públicos.
La firma de servidores públicos	El debate consiste en determinar si la firma de un servidor público que no hace constar un acto de autoridad debe considerarse pública, o bien, es un dato personal.

Fuente: Edgardo Martínez Rojas, *El derecho a la protección de datos personales en la Administración Pública Federal*.

4. Regulación del derecho de protección de datos en México

En el ámbito constitucional, a partir de una tesis aislada, se pueden identificar artículos de la Constitución Federal que regulan el derecho de protección de datos personales de forma detallada y que se vinculan con la protección de este derecho:

SISTEMAS DE PROTECCIÓN DE DATOS PERSONALES Y DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. PRECEPTOS CONSTITUCIONALES QUE LOS REGULAN

Si bien es cierto que el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos establece los principios, directrices y reglas básicas sobre las cuales se construyen los sistemas de protección de datos personales y de transparencia y acceso a la información pública, también lo es que en el propio Texto Constitucional se contienen otras reglas específicas al respecto, como ocurre tratán-

dose de la identidad y de los datos personales de las víctimas y ofendidos partes en el procedimiento penal (artículo 20, apartado C, fracción V), del régimen de telecomunicaciones (artículos tercero y octavo transitorios del decreto de reforma en la materia, publicado en el Diario Oficial de la Federación el 11 de junio de 2013), la fiscalización de recursos públicos ejercidos por personas privadas (artículo 79), la creación del Sistema Nacional de Información Estadística y Geográfica (artículo 26, apartado B), el registro público sobre deuda pública (artículo 73, fracción VIII, inciso 3o.), la investigación y sanción de responsabilidades administrativas y hechos de corrupción, tratándose de información fiscal o relacionada con el manejo de recursos monetarios (artículo 109, fracción IV), el Sistema de Información y Gestión Educativa (artículo quinto transitorio del decreto de reformas publicado en el señalado medio el 26 de febrero de 2013), la recopilación de información geológica y operativa a cargo de la Comisión Nacional de Hidrocarburos [artículo décimo transitorio, inciso b), del decreto de reformas constitucionales difundido el 20 de diciembre de 2013], el sistema de fiscalización sobre el origen y destino de los recursos de los partidos políticos, coaliciones y candidatos (artículo segundo transitorio del decreto de reformas publicado el 10 de febrero de 2014) y la fiscalización de la deuda pública (artículo séptimo transitorio del decreto que modifica diversas disposiciones constitucionales, publicado el 26 de mayo de 2015).²⁸

A partir de ello, se observa que el derecho de protección de datos personales incide en diversos ámbitos relacionados con aspectos de la vida de las personas y, por lo tanto, las responsabilidades del Estado en diversas materias, así como en las áreas en las que de conformidad con la tesis anteriormente citada, prevén que haya incidencia en el derecho a la protección de datos personales. Por ello, se debe poner especial cuidado en las telecomunicaciones, las responsabilidades administrativas, la fiscalización de recursos públicos ejercidos por personas privadas o bien aquellos correspondientes a partidos políticos y candidatos, el registro de deuda pública

²⁸ Tesis aislada: I.2o.A.E.1 CS (10a.), *Gaceta del Semanario Judicial de la Federación*, t. III, libro XXXIX, febrero de 2017, p. 2364.

y los sistemas de información, geológica, estadística, geográfica y educativa, en materia penal, para no vulnerar este derecho.

Por otra parte, en la legislación secundaria, la regulación del derecho a la protección de datos personales se bifurca en dos vertientes: información o datos en poder de la autoridad estatal e información en poder de los particulares.

Público

En el sector correspondiente a la información en poder de la autoridad estatal, y específicamente en el ámbito federal. La regulación se basa en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que se publicó el 9 de mayo de 2016 en el *Diario Oficial de la Federación*, y con la que se abrogó la anterior ley federal en la misma materia. Sin embargo, cabe señalar que también existe una ley general, cuyos contenidos no regulan la actuación de la autoridad en el ámbito federal, toda vez que la naturaleza de las leyes generales es la de ser un parámetro a partir del cual se despliegan las directrices en la materia que se trate, que deberán ser observadas por las entidades federativas en la legislación en la materia que cada una expida, como ejercicio de su autonomía.

Por su parte, la ley federal otorga al INAI la obligación de ser el organismo garante de ambos derechos y, en consecuencia, las facultades de los órganos y funcionarios específicos a cargo de la protección de ese derecho.

Sin embargo, la ley federal parece más abundante y específica respecto de la transparencia y acceso a la información, previendo incluso un capítulo titulado “Gobierno Abierto” y otro titulado “De las obligaciones de transparencia de los sujetos obligados”. Pese a que la ley no está argumentada con el mismo detalle en cuanto al derecho de protección de datos personales, no está exenta del peligro de incumplimiento de la obligación que tiene el Estado de prevenir y garantizar el ejercicio de éste.

Privado

Este sector se refiere a la regulación que se creó para regular la información en poder de personas privadas, lo cual había sido un ámbito ignorado debido a la renuencia a afirmar que la autoridad no sólo es aquella de *iure*, sino que hay autoridades de *facto* caracterizadas en personas particulares, y que ello implica la posibilidad de que también se vulneren los Derechos Humanos en su carácter de autoridad. Como consecuencia, la Ley Federal de Protección de Datos Personales en Posesión de Particulares se publicó en el *Diario Oficial de la Federación* hasta el 5 de julio de 2010.

El objetivo de la disposición *en comento* es “regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas”.²⁹

Como sujetos obligados, prevé a las sociedades crediticias y a todo particular que lleve a cabo la recolección y almacenamiento de datos personales, sin importar los medios o el fin. Además, se advierte como regla general que para todo tratamiento de datos personales se requiere el consentimiento del titular, que en ocasiones puede ser tácito y en otras se requiere la firma. De la misma forma, se prevén excepciones, como: datos personales que se encuentren en fuentes de acceso público, los que se sometan a procedimiento de disociación,³⁰ si existe una situación de emergencia que pueda dañar a un individuo en su persona o sus bienes, que se tenga como propósito cumplir obligaciones derivadas de una obligación jurídica, como resultado de una resolución por la autoridad competente o si son indispensables para la atención médica, prevención, diagnóstico, asistencia sanitaria o tratamientos relacionados a la salud.³¹

²⁹ Ley Federal de Protección de Datos Personales en Posesión de Particulares, Artículo 1, disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017> (consultado el 18 de abril de 2018).

³⁰ Procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir la identificación del mismo.

³¹ Ley Federal de Protección de Datos Personales en Posesión de Particulares, artículo 10, *ibid.*

Cabe mencionar que, en el caso de datos personales en poder de los particulares, el INAI es el órgano facultado para “difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia”.³²

La regulación mencionada podría mejorar la previsión del consentimiento tácito, a pesar de que la protección de datos personales es un derecho que, como ya se explicó en capítulos anteriores, tiene íntima relación con la privacidad de la persona, y por lo tanto el tratamiento de los datos personales incide directamente en la esfera de derechos, así como en el desarrollo y la calidad de vida de las personas. Pareciera ser que no es tan conveniente un consentimiento tácito, menos aun cuando la propia ley lo reconoce como un requisito o supuesto que no es excepcional.

5. Principios y deberes en los datos personales

Estos principios garantizan la seguridad y el buen manejo de la información de cada individuo.

<i>Principio</i>	<i>Descripción</i>
De consentimiento	El principio de consentimiento requiere de la manifestación del titular para dar a conocer la información de manera libre, informada y específica.
De licitud	En el principio de licitud, el responsable deberá tratar los datos de cada individuo conforme a la normatividad aplicable, respetando lo acordado entre el responsable y el titular. Se requiere que el responsable tenga que adoptar medidas para asegurar el tratamiento de los datos personales, que se hará con pleno cumplimiento de la legalidad, respeto de la buena fe y respeto de los derechos del individuo.

³² Ley Federal de Protección de Datos Personales en Posesión de Particulares, artículo 38, *ibid.*

<i>Principio</i>	<i>Descripción</i>
De proporcionalidad	Según el principio de proporcionalidad, el titular debe recabar sólo la información necesaria para el cumplimiento de sus fines.
De finalidad	Dentro del principio de finalidad, los datos personales sólo deben limitarse al cumplimiento de las finalidades determinadas.
De calidad	De acuerdo con el principio de calidad, la información deberá ser cierta y actualizada para el cumplimiento de sus fines. Ésta deberá ser suprimida una vez que se cumplan o agoten las finalidades para las cuales fue recabada.
De información	En el principio de información, el responsable tendrá que informar al titular sobre qué datos personales obtiene y qué finalidad tienen.
De responsabilidad	Para que el principio de responsabilidad se efectúe de manera adecuada, el responsable que posee la información personal de cada individuo está obligado a protegerla.

Fuente: Elaboración propia.

En cuanto a los deberes, la siguiente lista representa aquellos que deben respetarse a cabalidad, según la ley.

- Deber de seguridad: tiene como finalidad proteger los datos personales contra su acceso no autorizado a través de medidas de seguridad técnicas, físicas y administrativas, mismas que también protegen los datos personales contra daño, pérdida, alteración o destrucción.
- Deber de confidencialidad: el responsable está obligado a guardar en secreto los datos personales del titular, no deberá divulgarlos o ponerlos a disposición de terceros, ni mucho menos utilizarlos para otros propósitos que no sean aquellos para los cuales se obtuvieron.

6. Tipos de datos personales

De conformidad con el artículo 3, fracción segunda, de la Ley Federal de Transparencia y Acceso a la Información Pública:

Un dato personal es la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas.

De esta manera, se puede afirmar que los datos personales engloban la información propia de cada individuo, la cual nos distingue de los demás, por ejemplo:³³

- Datos de identificación y contacto
- Datos laborales
- Datos académicos
- Datos sobre pasatiempos, entretenimiento y diversión
- Datos migratorios

Por otra parte, existen también aquellos datos que son más delicados, llamados “sensibles”, que afectan 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 o preferencia sexual, además de:

- Datos biométricos
- Datos legales

³³ Una definición más extensa puede verse en el apartado “Glosario” de este libro, p. 76.

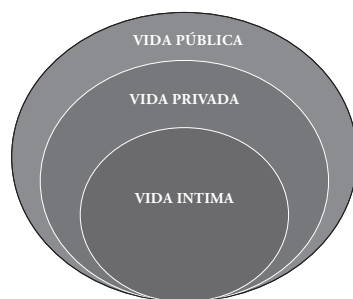
- Datos sobre señas particulares
- Datos específicos sobre la vida sexual
- Datos sobre características físicas

Por último, los datos abiertos son diversos tipos de datos libres de usar, reutilizar y redistribuir, sin ninguna restricción legal, tecnológica o social. Cuando los datos abiertos se convierten en información útil, utilizable y utilizada se les conoce como contenido abierto.

Las principales características de los datos abiertos son:

- La disponibilidad y acceso, es decir, que los datos estén disponibles en su conjunto, principalmente a través de internet, de forma completa y modificable.
- Reutilización y redistribución, referido a que los datos deben ser proporcionados en condiciones que permitan su reuso, reutilización y redistribución.
- Participación universal, es decir, que cada interesado debe ser capaz de utilizar, reutilizar y redistribuir los datos, sin ningún tipo de limitaciones o restricciones de uso por parte de personas o grupos.³⁴

Esquema de protección



Fuente: Elaboración propia.

³⁴ Valeria Salas y Eduardo Rubio, *Estudio sobre el valor económico de los datos personales*, Secretaría de Economía/AIMPDI, disponible en <https://asociacion-deinternet.mx/images/valor_eco_Datospersonales_FINAL.pdf> (consultado el 3 de abril de 2018).

II. LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

Esta ley fue publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017, la cual dicta la obligación exclusiva, en el ámbito federal, estatal y municipal, que tiene cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de proteger los datos personales.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados es de orden público y de observancia general en toda la República, además de ser reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.

Los sujetos obligados son, en el ámbito federal, estatal y municipal, como ya se había mencionado, cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Dicha ley es aplicable a los datos personales que estén en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. El consentimiento puede expresarse de dos formas: expresa y tácita. Este último se deberá hacer verbalmente, por escrito o por cualquier medio con signos inequívocos. Mientras que según el consentimiento tácito, el propio titular manifestará su voluntad, según corresponda.

Existe una excepción respecto a los datos personales sensibles, en la que el titular deberá expresar su voluntad de manera expresa y por escrito mediante firma autógrafa, electrónica u otro medio de autenticidad.

1. Sanciones por el incumplimiento de obligaciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Estas sanciones serán causadas por:

- Actuar con negligencia, dolo o mala fe durante la substanciación de las solicitudes para el ejercicio de los derechos.
- Incumplir los plazos para responder las solicitudes para el ejercicio de los derechos o para hacer efectivo el derecho de que se trate.
- Hacer el mal uso de datos personales que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.
- Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes.
- No contar con el aviso de privacidad.
- Incumplir el deber de confidencialidad.
- No establecer las medidas de seguridad.
- Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad.
- Llevar a cabo la transferencia de datos personales afectando al titular de los datos personales.
- Obstruir los actos de verificación de la autoridad.
- No acatar las resoluciones emitidas por el instituto y los organismos garantes.

2. Aviso de privacidad

Es un documento impreso, digital, visual o sonoro en el que se establecen los datos personales de cada individuo, y en el cual se informa qué tipos de datos son y cuáles son sus fines. El responsable tiene la obligación de informarle a cada titular sobre éstos.

El aviso de privacidad deberá contener:

- Identidad y domicilio del responsable que los recaba.
- Finalidades del tratamiento de datos.
- Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos.
- Medios para ejercer los derechos de acceso, rectificación, cancelación u oposición.
- En su caso, las transferencias de datos que se efectúen.
- El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad.

Modelos de avisos de privacidad

Modelo A. Aviso de privacidad integral:

El aviso de privacidad integral deberá contener:

- I. La identidad y el domicilio del responsable que trata los datos personales.
- II. Los datos personales que serán sometidos a tratamiento.
- III. El señalamiento expreso de los datos personales sensibles que se tratarán.
- IV. Las finalidades del tratamiento.
- V. Los mecanismos para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el responsable.
- VI. Las transferencias de datos personales que, en su caso, se efectúen; el tercero receptor de los datos personales, y las finalidades de las mismas.
- VII. La cláusula que indique si el titular acepta o no la transferencia, cuando así se requiera.
- VIII. Los medios y el procedimiento para ejercer los derechos ARCO.

- IX. Los mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de sus datos personales.
- X. Las opciones y medios que el responsable ofrece al titular para limitar el uso o la divulgación de los datos personales.
- XI. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso.
- XII. Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.³⁵

Modelo B. Aviso de privacidad simplificado:

El aviso de privacidad simplificado deberá contener, al menos, la siguiente información.

- I. La identidad y el domicilio del responsable.
- II. Las finalidades del tratamiento.
- III. Los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad integral.

Modelo C. Aviso de privacidad corto

Al igual que el aviso de privacidad simplificado el aviso de privacidad corto deberá contener.

- I. La identidad y domicilio del responsable.
- II. Las finalidades del tratamiento.
- III. Los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad integral.³⁶

³⁵ “Guía para el Aviso de Privacidad”, IFAI, disponible en <<http://inicio.ifai.org.mx/SitePages/Guia-para-el-Aviso-de-Privacidad.aspx>> (consultado el 3 de abril de 2018).

³⁶ “Lineamientos del Aviso de Privacidad”, DOF, disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013> (consultado el 3 de abril de 2018).

III. DERECHOS ARCO

Las siglas ARCO se desglosan de la siguiente manera:

- Acceso: el titular de los datos puede conocer qué información personal posee alguna empresa.
- Ratificación: el titular puede pedir a la empresa que se modifiquen algunos datos sobre él.
- Cancelación: el titular puede solicitar que se borren los datos que están registrados.
- Oposición: el titular de los datos puede presentar una queja por el uso que se le está dando a su información personal.

Para ejercer estos derechos es indispensable acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante. Los derechos ARCO se podrán ejercer de manera excepcional cuando se trate de una disposición legal o mandato judicial.

Aun cuando las personas fallezcan, se pueden ejercer estos derechos a través de otra persona que acredite tener un interés jurídico, siempre y cuando el titular del derecho hubiera expresado esta voluntad o, en su caso, exista un mandato judicial. En ambos casos, ejercer estos derechos deberá ser de manera gratuita, a menos de que se necesite hacer una reproducción, certificación o envío, pues se realizará un cobro para la recuperación de los gastos.

Para ejercer estos derechos se debe presentar una solicitud con la siguiente información:

- El nombre del titular y su domicilio.
- Documentos que acrediten la identidad o, en su caso, la representación legal del titular.
- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer sobre alguno de los derechos antes mencionados.

Posteriormente, el responsable tiene un plazo de 20 días contados desde la fecha en que se recibió dicha solicitud para dar

respuesta. En caso de ser procedente se hará efectiva la misma en quince días posteriores.

El responsable podrá negar el acceso a los datos personales y ejercer sus derechos cuando:

- El solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado.
- En su base de datos no se encuentren los datos personales del solicitante.
- Se lesionen los derechos de un tercero.
- Exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos.
- La rectificación, cancelación u oposición haya sido previamente realizada.

La Suprema Corte de Justicia de la Nación (SCJN) ha establecido órganos para garantizar estos derechos respecto a la publicación de datos personales:

<i>Órgano</i>	<i>Descripción</i>
Comité Especializado	Está conformado por tres ministros, mismos que son nombrados por el pleno. Se encargan de supervisar y cumplir con las disposiciones constitucionales en materia de transparencia, acceso a la información pública y protección de datos personales por parte de los servidores públicos de la SCJN.
Comité de Transparencia	Se integra por servidores públicos de la SCJN y es la instancia ejecutiva encargada de tomar las medidas necesarias para coordinar las acciones tendentes a cumplir con la publicidad, acceso a la información y protección de datos personales.

<i>Órgano</i>	<i>Descripción</i>
La Unidad General de Transparencia y Sistematización de la Información Judicial	Se encarga de publicitar la información y de dar trámite a las solicitudes de acceso a la información, así como a las de rectificación, cancelación u oposición a la publicación de datos personales.
Módulos de Acceso	Son los órganos administrativos dependientes de la Unidad General de Transparencia y Sistematización de la Información Judicial, encargados de recibir las solicitudes de acceso a la información, rectificación, cancelación u oposición.

Fuente: Elaboración propia.

1. *Requisitos de la solicitud para ejercer los derechos ARCO en la publicación de datos personales*

- Nombre del interesado, representante legal y tutor, así como el documento que acredite su representación.
- La expresión y acreditación de su interés.
- El nombre del tercero interesado, si lo hubiere.
- El señalamiento, con la mayor precisión posible, del nombre y ubicación del archivo o registro de datos, así como del órgano del cual depende.
- La precisión de los datos personales que son materia de la solicitud de acceso, rectificación, cancelación u oposición a su publicación.
- Las razones por las que considera que el registro o archivo de datos señalados resulta discriminatoria, de riesgo para su integridad, falsa o inexacta.
- De manera opcional, la solicitud de anotación provisional en el archivo o registro de datos, relativa a que la información cuestionada está sometida a un proceso administrativo de corrección.
- En su caso, las pruebas que acrediten sus pretensiones.
- Firma del promovente, su representante o de quien lo haga a su ruego, si se encuentra imposibilitado para ello.

La Unidad General de Transparencia y Sistematización de la Información Judicial podrá requerir al solicitante, por única ocasión, advertir alguna deficiencia en su escrito y tendrá un plazo de tres días hábiles para que la precise o modifique.

2. Medios de defensa para solicitar inconformidad

1) A petición del titular

Se interpone ante el Comité de Transparencia, por conducto de la Unidad General de Transparencia y Sistematización de la Información Judicial, o ante cualquier Módulo de Acceso, dentro de los siguientes 10 días hábiles en que reciba la notificación.

Este medio de defensa deberá resolverse en un plazo de 20 días hábiles, prorrogable únicamente hasta por 15 días hábiles y deberá ser considerado por el comité.

b) Recurso de Revisión

Se analiza y resuelve por el Comité Especializado, y procede contra las resoluciones del Comité de Transparencia, en las que:

- No se entreguen al solicitante los datos personales solicitados o se haga en un formato incomprensible.
- Exista negativa de efectuar modificaciones o correcciones a los datos personales.
- El solicitante no esté conforme con el tiempo o la modalidad de entrega de los datos personales.
- El solicitante considere que los datos personales entregados son incompletos o no correspondan a los requeridos en su solicitud.

Este recurso deberá resolverse en un plazo de 50 días hábiles, prorrogables por un periodo.

c) Recurso de reconsideración

Este medio de defensa se puede interponer una vez que haya transcurrido un año a partir de que el Comité Especializado emitió la resolución que confirma la decisión del Comité de Transparencia. Tiene por objeto solicitar al Comité Especializado que reconsidere su resolución o criterio.

Este recurso permite que de oficio se revise lo siguiente:

Procedimiento de supervisión

El Comité de Transparencia se encargará de este procedimiento para vigilar el cumplimiento correcto de las obligaciones de transparencia y protección de datos personales a cargo de los servidores públicos de la Suprema Corte.

Procedimiento de ejecución

El Comité de Transparencia conocerá este procedimiento para cotejar el cumplimiento de sus resoluciones por parte del órgano obligado en las resoluciones de *hábeas data* y supervisión.

Incidente de incumplimiento

El Comité Especializado lo analiza y resuelve, y tendrá a su cargo asegurar la ejecución de sus resoluciones y las del Comité de Transparencia, en las que el órgano responsable no hubiese cumplido con las obligaciones impuestas en las resoluciones respectivas.

3. *Transferencia nacional e internacional de datos personales*

La transferencia internacional tiene lugar cuando los datos personales salen del territorio de un país e ingresan al territorio de otro Estado.

Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá

comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.³⁷

Estas transferencias se harán sin el consentimiento del titular cuando:

- exista previsión en una ley o tratado del que México sea parte.
- la transferencia sea necesaria para la prevención o el diagnóstico médico.
- la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas.
- la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.
- la transferencia sea necesaria o legalmente exigida para salvaguardar un interés público, o para la procuración o administración de justicia.
- la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

IV. DERECHO INFORMÁTICO

En la actualidad, dentro de la administración pública existe un crecimiento extraordinario en el volumen y la complejidad de actividades de las dependencias gubernamentales debido, entre otras cosas, al pronunciado desarrollo demográfico, económico y tecnológico, que ha obligado a que dicho sector, en sus diferentes niveles (federal, estatal y municipal), esté cada vez más capacitado para recibir, tramitar, analizar y difundir todo tipo de información jurídica para su correcto funcionamiento.

³⁷ Ley Federal de Protección de Datos Personales en Posesión de los Particulares, artículo 36, *ibid*.

Mediante la adecuada aplicación de la informática jurídica de control y gestión, se puede lograr una mejora sustancial de las estructuras jurídico-administrativas, así como de los sistemas de operación. Esto es una medida indispensable para que las entidades del sector público, a través de los poderes Ejecutivo, Legislativo y Judicial, alcancen sus objetivos sociales apoyados en la utilización de la tecnología moderna.³⁸

El derecho informático es el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones.

Es importante estudiar el tema, pues a lo largo de nuestra vida proporcionamos datos personales a instituciones públicas o privadas con el fin de facilitar un servicio determinado con mayor eficacia. Actualmente, estas instituciones tienen mejor manejo de dicha información, gracias a las técnicas informativas y a la transmisión de datos entre ordenadores. Toda la información personal que está organizada mediante sistemas de almacenamiento debe estar protegida contra el acceso de personas que no están autorizadas.

Los datos personales pueden ser públicos o privados. Estos últimos se dividen en íntimos y secretos. Y los secretos en profundos o reservados. Los datos personales públicos son conocidos por cualquier persona, incluso sin que el titular pueda saber; un ejemplo de ellos son el nombre, el apellido y la edad. Bajo este mismo tenor, se exponen los siguientes conceptos y definiciones.

- Datos personales privados: el titular de la información debe dar su consentimiento y se debe respetar su privacidad.
- Datos personales íntimos: son aquellos que puede proteger la misma persona que los ostenta frente a terceros, pero no puede oponerse cuando se requieran ante algún mandato legal.
- Datos personales secretos: son los que están reservados a la ideología o creencias. El individuo no está obligado a proporcionarlos salvo a excepciones, por ejemplo, hablar sólo en presencia de un abogado. Los datos secretos también podrían considerarse como profundos, por ejemplo, la salud, las preferencias sexuales, etcétera.

³⁸ Julio Téllez Valdés, *Derecho informático*, México, McGraw-Hill, 1996, p. 43.

1. *Sitios web y redes sociales que vulneran la protección de datos personales*

Existen dos tipos de redes sociales, *online* y *offline*, así como las redes sociales digitales y los servicios de redes sociales. Las redes *online* se definen como servicios prestados a través de internet que permiten a los usuarios generar un perfil público en el que suben y bajan información, a la vez que posibilitan la interacción con el resto de usuarios. Las redes *offline* son aquellas en las que las relaciones sociales, con independencia de su origen, se desarrollan sin mediación de aparatos o sistemas electrónicos.

Las redes sociales digitales son las plataformas de intercambio de información basadas en perfiles, como Facebook o Twitter. Los servicios de redes sociales, mejor conocidos como empresas, habilitan el espacio virtual necesario y ponen a disposición de los miembros en las redes los instrumentos tecnológicos exigidos para su desarrollo.³⁹

Prácticamente, la información que se sube a dichas plataformas es pública, pues el usuario acepta los términos y condiciones para subir sus fotos, videos e incluso su ubicación. Una recomendación para proteger la información es no comunicar datos personales, como domicilio, lugar de trabajo, ocupación. De igual manera, es recomendable sólo aceptar solicitudes de amistad de gente conocida, además de resguardar la contraseña y personalizar la privacidad en las redes sociales, mismas que permiten decidir quién puede acceder a las partes específicas de los distintos perfiles.

En México han ido al alza en cuanto a tecnología, en específico el internet, pues según los datos de Ilifebelt, México se perfila a llegar a 61 millones de usuarios es este año. (2018)

De acuerdo a un estudio de hábitos del usuario, el 51% de los que consumen internet son mujeres, y el 49% hombres. La edad que más consume esta herramienta oscila entre los 6 y 34 años.

³⁹ Hermina Campuzano Tomé, “Las redes sociales digitales: concepto, clases y problemática jurídica que plantean en los albores del siglo xxi”, *Revista Actualidad Civil*, España, núm. 1, 2011. p.19.

Ahora bien, teniendo la tecnología al alcance de la mano, los mexicanos utilizan diferentes aplicaciones para chatear, interactuar, escuchar música o ver películas. Todo esto lo hacen a través de un teléfono inteligente. De acuerdo con datos de la Asociación de Internet, el 90% de la población utiliza el smartphone.

Estas son las aplicaciones más utilizadas en México:

- Facebook 95%
- WhatsApp 93%
- Twitter 66%
- Instagram 59%
- Snapchat 31 %
- Swarm 9%⁴⁰

En la actualidad, es común que una persona utilice alguna red social que vulnera los datos personales, aunque sea muy poca la información que se sube. Utilizar nombre, sexo, edad o el lugar donde se reside fragmenta la seguridad jurídica.

CONCLUSIONES

El derecho de protección de datos personales se suma al elenco de los Derechos Humanos, clasificado como derecho de primera generación, por lo que conlleva la obligación de no hacer, que resulta exigible a la autoridad.

En esa línea de ideas, se ha admitido recientemente en nuestro sistema jurídico que la autoridad no sólo es aquella que está reconocida *de iure* y formalmente, es decir, aquella que pertenece al Estado, sino que el concepto se ha ampliado para abarcar a la autoridad *de facto* que no es parte de la estructura institucional del gobierno, pero ejerce atribuciones como si fuera la autoridad, y dado el riesgo de que vulnere Derechos Humanos, también le importan las obligaciones en dicha materia que son propias de la autoridad.

⁴⁰ “Las aplicaciones más usadas en México”, en *El Universal*, 30 de enero del 2018, disponible en <<http://www.eluniversal.com.mx/techbit/las-aplicaciones-mas-usadas-en-mexico>> (consultado el 3 de abril de 2018).

Lo anterior es un factor que influye en cómo se aborda el derecho a la protección de datos personales en México. Así, la regulación del mismo se desenvuelve escasamente en la Constitución Federal y en la legislación secundaria se despliega en dos vertientes: aquella que regula la protección de datos personales respecto de la autoridad gubernamental y aquella que regula la protección a los mismos datos en posesión de los particulares.

Además, debe considerarse la amenaza latente al derecho a la protección de datos personales, que constituye el vertiginoso cambio tecnológico y con ello la modernización en los medios de comunicación y la transformación en la manera en que fluye la información de toda índole.

Resulta evidente que uno de los Derechos Humanos que en ocasiones pudiera entrar en colisión con el de protección de datos personales es el de acceso a la información, cuya regla general es la publicidad y la excepción es la reserva. Sin embargo, ello no supone que el acceso a la información siempre sea el derecho que prevalezca, sino que hay que tener en cuenta que ambos son Derechos Humanos y, por consiguiente, cada uno tiene límites, cuyo supuesto deberá ser valorado en cada situación específica.

FUENTES CONSULTADAS

Bibliográficas

- ARAUJO CARRANZA, Ernesto, *El Derecho a la Información y Protección de Datos Personales en México*, México, Porrúa, 2009.
- BAJO FERNÁNDEZ, Miguel, “Protección del honor y de la intimidad”, en *Comentarios a la legislación penal*, M. Cobo del Rosal (dir.), t. I, Madrid, Derecho Penal y Constitución, 1982.
- CELIS QUINTAL, Marcos Alejandro, “La protección de la intimidad como derecho fundamental de los mexicanos”, en *Estudios en homenaje a Marcia Muñoz de Alba Medrano. Protección de la persona y derechos fundamentales*, Cienfuegos Salgado David y Macías Vázquez María Carmen (coords.), México, UNAM-IIJ (Serie doctrinaria) 324, 2006.

- CONDE COLMENTERO, Pilar *et al.*, *Los derechos a la intimidad y a la privacidad en el siglo XXI*, España, Dykinson, 2011.
- DESANTES GUANTER, José María, *Derecho a la información. Materiales para un sistema de la comunicación*, Valencia, Fundación COSO, 2004.
- MUÑOZ DE ALBA MEDRANO, Marcia y Alberto Cano Valle, *Derechos de las personas con Síndrome de Inmunodeficiencia Adquirida*, México, Cámara de Diputados/UNAM, 2002.
- PIÑAR, José Luis (coord.), *Transparencia, acceso a la información y protección de datos*, Madrid, Reus, 2014.
- TÉLLEZ Valdés, Julio, *Derecho informático*, México, McGraw-Hill, 1996.
- TOBÓN Franco, Natalia, *Libertad de expresión y derecho de autor. Guía legal para periodistas*, Bogotá, Universidad del Rosario, Colegio Mayor de Nuestra Señora del Rosario-Facultad de Jurisprudencia, 2009.
- WESTIN, Alan F., *Privacy and Freedom*, Nueva York, Atheneum, 1970.

Hemerográficas

- CAMPUZANO TOMÉ, Hermina, “Las redes sociales digitales: concepto, clases y problemática jurídica que plantean en los albores del siglo XXI”, *Revista Actualidad Civil*, España, núm. 1, 2011. p.19.
- GARZÓN VALDÉZ, Ernesto, “Lo íntimo, lo privado y lo público”, *Claves de la razón práctica*, núm. 137, noviembre de 2003.
- HERRERA BRAVO, Rodolfo, “La protección de datos personales como garantía básica de los Derechos Fundamentales”, *Derechos Humanos*, núm. 71, Comisión de Derechos Humanos del Estado de México, enero-febrero 2005.
- NIEVES SALDAÑA, María, “The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis”, *Revista de Derecho Político*, núm. 85, septiembre-diciembre 2012.

- SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, *Criterios del Poder Judicial de la Federación en materia de protección de datos personales y otros conceptos relacionados*, segunda edición, México, Suprema Corte de Justicia de la Nación, 2016
- Tesis 1a. CCXVII/2013 Primera Sala, *Gaceta del Semanario Judicial de la Federación*, t. I, libro XXII, julio de 2013.
- Tesis 1a. CII/2015 (10a.) Primera Sala, *Gaceta del Semanario Judicial de la Federación*, t. II, libro 16, marzo de 2015.
- Tesis 1a. VII/2012, Registro: 2000233, Primera Sala, *Gaceta del Semanario Judicial de la Federación*, t. I, libro V, febrero de 2012.
- Tesis aislada 1a. XLIII/2010, *Gaceta del Semanario Judicial de la Federación*, t. XXXI, marzo de 2010.
- Tesis aislada: I.4º. A.17 K (10a.), *Gaceta del Semanario Judicial de la Federación*, t. III, libro XIX, abril de 2012.
- Tesis de jurisprudencia 32/2013 (10a.), *Gaceta del Semanario Judicial de la Federación*, t. I, libro XIX, abril de 2013.
- Tesis II.1o.29 P (10a.), *Gaceta del Semanario Judicial de la Federación*, t. II, libro XX, México, Tribunales Colegiados de Circuito, julio de 2015.
- Tesis P./J. 25/2007, *Gaceta del Semanario Judicial de la Federación*, t. XXV, mayo de 2007.
- Tesis P./J. 54/2008, *Gaceta del Semanario Judicial de la Federación*, t. XXVII, junio de 2008.
- Tesis: III.1o.C.1 K, Registro: 2006639, *Gaceta del Semanario Judicial de la Federación*, t. II, libro VII, Tribunales Colegiados de Circuito, junio de 2014.

Electrónicas

- Constitución Política de los Estados Unidos Mexicanos, disponible en: <http://www.sct.gob.mx/JURE/doc/cpeum.pdf>
- Declaración Universal de Derechos Humanos, p.26. Disponible en <http://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf> (consultado 27 de Junio de 2018).

“Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados”, *DOF*, disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017> (consultado 27 de Junio de 2018).

“Decreto por el que se abroga la Ley Federal de Transparencia y Acceso a la Información Pública Pública Gubernamental”, *DOF*, disponible en <http://www.dof.gob.mx/avisos/2493/SG_090516/SG_090516.html> (consultado 27 de Junio de 2018).

“El derecho de acceso a la información es un derecho fundamental”, *Comunidad Baratz*, 28 de octubre de 2016, disponible en <<http://www.comunidadbaratz.com/blog/el-derecho-de-acceso-a-la-informacion-es-un-derecho-fundamental/>> (consultado 27 de Junio de 2018).

“Guía para el Aviso de Privacidad”, *IFAI*, disponible en <<http://inicio.ifai.org.mx/SitePages/Guia-para-el-Aviso-de-Privacidad.aspx>> (consultado 27 de Junio de 2018).

“Las aplicaciones más usadas en México”, *El Universal*, 30 de enero del 2018, disponible en <<http://www.eluniversal.com.mx/techbit/las-aplicaciones-mas-usadas-en-mexico>> (consultado 27 de Junio de 2018).

“Lineamientos del Aviso de Privacidad”, *DOF*, disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013> (consultado 27 de Junio de 2018).

MARTÍNEZ ROJAS, Edgardo, *El derecho a la protección de datos personales en la Administración Pública Federal*, México, IFAI, 2011, disponible en <https://www.itei.org.mx/v3/micrositios/diplomado02/gdl/adjuntos/Sector_Publico ITEI_18-19-nov-2011.pdf> (consultado 27 de Junio de 2018).

SALAS, Valeria y Eduardo Rubio, *Estudio sobre el valor económico de los datos personales*, Secretaría de Economía/AIMPCI, disponible en <https://asociaciondeinternet.mx/images/valor_eco_Datospersonales_FINAL.pdf> (consultado 27 de Junio de 2018).

VÉLEZ Campos, Nadia, *Protección de datos personales en México*, tesis de maestría, Universidad de las Américas, Puebla, disponible en <http://catarina.udlap.mx/u_dl_a/tales/documentos/mco/velez_c_n/portada.html> (consultado 27 de Junio de 2018).