

EXPEDIENTE: 01027/INFOEM/IP/RR/2014

SUJETO OBLIGADO: AYUNTAMIENTO DE TENANGO DEL  
VALLE

COMISIONADA PONENTE: EVA ABAID YAPUR

VOTO EN CONTRA DE: FEDERICO GUZMÁN TAMAYO.

## VOTO EN CONTRA

Con relación al Recurso de Revisión identificado con el número 1027/INFOEM/IP/RR/2014, en contra del **AYUNTAMIENTO DE TENANGO DEL VALLE**, que fuera turnado a la Comisionada **EVA ABAID YAPUR**, se emite el siguiente **VOTO EN CONTRA** en virtud de que en la resolución se determinó como inoperantes los agravios aducidos por el **RECURRENTE**.

Como es posible observar la **PONENTE** estima que respecto los motivos de inconformidad del recurrente respecto que **SOLICITO QUE EL PRESENTE RECURSO DE REVISIÓN SE ENDERECE COMO DENUNCIA TODA VEZ QUE LA RESPUESTA CONTENIDA EN EL ARCHIVO EN COMENTO VIOLA EN TODOS SENTIDOS LO DISCURSO EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO**, mismo que la **PONENTE** considera como agravio inoperante, motivo por el cual desecha el recurso de revisión, no obstante para el suscrito se difiere de dicho criterio.

A efecto de desarrollar lo anterior es oportuno acotar que el artículo 1 de la Ley de Protección de Datos Personales del Estado de México, establece como uno sus objetos el de "... proteger los datos personales que se encuentre en posesión de los sujetos obligados, en esta tesis, sobre la protección a los datos personales resulta pertinente traer a colación lo previsto por la Ley:

### *Del Objeto de la Ley*

**Artículo 1.-** La presente Ley es de orden público, de interés social y de observancia general en todo el territorio del Estado de México, y tiene por objeto, garantizar la protección de los datos personales que se encuentran en posesión de los sujetos obligados así como establecer los principios, derechos, excepciones, obligaciones, sanciones y responsabilidades que rigen en la materia.

### *De la Finalidad de la Ley*

**Artículo 2.-** Son finalidades de la presente Ley:

**I. Garantizar la observancia de los principios** de protección de datos personales en posesión de los sujetos obligados;

**II. Proveer lo necesario para que toda persona pueda ejercer los derechos de acceso, rectificación y cancelación de sus datos personales, así como manifestar su oposición a determinado tratamiento, mediante procedimientos sencillos y expeditos;**

**III. Promover la adopción de medidas de seguridad que garanticen la integridad, disponibilidad y confidencialidad** de los datos personales en posesión de los sujetos obligados.

*De los Sujetos Obligados*

*Artículo 3.- Son sujetos obligados para la aplicación de esta Ley, los siguientes:*

*I. El Poder Ejecutivo;*

*II. El Poder Legislativo;*

*III. El Poder Judicial;*

***IV. Los Ayuntamientos;***

*V. Los Órganos y Organismos Constitucionales Autónomos; y*

*VI. Los Tribunales Administrativos.*

*Glosario*

*Artículo 4.- Para los efectos de esta Ley se entiende por:*

*I. a VI. (...)*

***VII. Datos personales: Cualquier información concerniente a una persona física identificada o identificable;***

***VIII. Datos personales sensibles: Aquellos que afectan 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 aquellos que puedan revelar aspectos como origen étnico o racial; información de salud física o mental, información genética, datos biométricos, firma electrónica, creencias religiosas, filosóficas o morales; afiliación sindical; opiniones políticas y preferencia sexual;

***IX. Derechos ARCO: Los Derechos de Acceso, Rectificación, Cancelación y Oposición de datos personales;***

*X a XXIV. (...)*

***XXV. Titular: Persona física a quien corresponden los datos personales que sean objeto de tratamiento;***

*XXVI. a XXX. (...)*

*Derechos*

*Artículo 25.- Los derechos de acceso, rectificación, cancelación y oposición de datos personales son derechos independientes. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. La procedencia de estos derechos, en su*

EXPEDIENTE: 01027/INFOEM/IP/RR/2014  
SUJETO OBLIGADO: AYUNTAMIENTO DE TENANGO DEL  
VALLE  
COMISIONADA PONENTE: EVA ABAID YAPUR

VOTO EN CONTRA DE: FEDERICO GUZMÁN TAMAYO.

*caso, se hará efectiva una vez que el titular o su representante legal acrediten su identidad o representación, respectivamente.*

#### **Derecho de Acceso**

**Artículo 26.-** *El titular tiene derecho a solicitar y ser informado sobre sus datos personales que estén en posesión del sujeto obligado, el origen de dichos datos, el tratamiento del cual sean objeto, las cesiones realizadas o que se pretendan realizar, así como a tener acceso al aviso de privacidad al que está sujeto el tratamiento, en los términos previstos en la ley.*

*El responsable del tratamiento, debe responder al ejercicio del derecho de acceso, tenga o no datos de carácter personal del interesado en su sistema de datos.*

#### **Derecho del Titular a Presentar Denuncias**

**Artículo 32.-** *El titular de los datos podrá denunciar ante el Instituto por posibles violaciones a las disposiciones establecidas en esta Ley, a fin de que se proceda a realizar la investigación respectiva y en su momento a emitir la resolución que en derecho proceda.*

*Asimismo, en caso de que el Instituto tenga conocimiento, por cualquier otro medio, de posibles violaciones a las disposiciones de la Ley o los lineamientos, podrá iniciar de oficio la investigación respectiva.*

*Las denuncias serán tramitadas en términos del procedimiento aprobado por el Instituto.*

*Cuando derivado de la investigación de los casos de violación del derecho a la protección de datos personales, se desprenda que puede existir menoscabo de otros derechos humanos correlativos, el Instituto se coordinará con las instancias u organismos competentes, para la investigación correspondiente, con la finalidad de garantizar cabalmente la protección integral de dichos derechos humanos.*

#### **Título Sexto**

#### **De la Seguridad de los Datos Personales**

##### **Capítulo Primero**

##### **Medidas de Seguridad**

**Artículo 58.-** *Los sujetos obligados deberán adoptar, mantener y documentar las medidas de seguridad administrativa, física y técnica necesarias para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, mediante acciones que eviten su daño, alteración, pérdida, destrucción, o el uso, transmisión y acceso no autorizado, de conformidad con lo dispuesto en los lineamientos que al efecto se expidan.*

Dichas medidas serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales, deberán constar por escrito y ser comunicadas al Instituto para su registro.

Las medidas de seguridad que al efecto se establezcan deberán indicar el nombre y cargo del servidor público responsable o, en su caso, la persona física o jurídica colectiva que intervengan en el tratamiento de datos personales con el carácter de responsable del sistema de datos personales o usuario, según corresponda. Cuando se trate de usuarios se deberán incluir los datos del acto jurídico mediante el cual, el sujeto obligado otorgó el tratamiento del sistema de datos personales.

En el supuesto de actualización de estos datos, la modificación respectiva deberá notificarse al Instituto, dentro de los treinta días hábiles siguientes a la fecha en que se efectuó.

**Tipos y Niveles de Seguridad**

**Artículo 59.-** El sujeto obligado responsable de la tutela y tratamiento del sistema de datos personales, adoptará las medidas de seguridad, conforme a lo siguiente:

**A. Tipos de seguridad:**

**I. Física.**- Se refiere a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor;

**II. Lógica.**- Se refiere a las medidas de protección que permiten la identificación y autenticación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función;

**III. De desarrollo y aplicaciones.**- Corresponde a las autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas;

**IV. De cifrado.**- Consiste en la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integralidad y confidencialidad de la información; y

**V. De comunicaciones y redes.**- Se refiere a las restricciones preventivas y/o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

**B. Niveles de seguridad:**

**I. Básico.** - Se entenderá como tal, el relativo a las medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas de datos personales. Dichas medidas corresponden a los siguientes aspectos:

- a) Documento de seguridad;
- b) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;
- c) Registro de incidencias;
- d) Identificación y autenticación;
- e) Control de acceso;
- f) Gestión de soportes; y
- g) Copias de respaldo y recuperación.

**II. Medio.** - Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos:

- a) Responsable de seguridad;
- b) Auditoría;
- c) Control de acceso físico; y
- d) Pruebas con datos reales.

**III. Alto.** - Corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos. Los sistemas de datos a los que corresponde adoptar el nivel de seguridad alto, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

- a) Distribución de soportes;
- b) Registro de acceso; y
- c) Telecomunicaciones.

Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información.

#### **Naturaleza y registro de las medidas de seguridad**

Instituto de Transparencia, Acceso a la Información Pública y  
Protección de Datos Personales del Estado de México y Municipios

**Artículo 60.- Las medidas de seguridad a las que se refiere el artículo anterior constituyen mínimos exigibles, por lo que el sujeto obligado adoptará las medidas adicionales que estime necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de datos personales. Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará al Instituto, para su registro, el nivel de seguridad aplicable.**

De los preceptos legales transcritos, se desprende lo siguiente:

- Que la Ley de Protección de Datos Personales del Estado de México es de orden público, de interés social y de observancia general en todo el territorio del Estado de México, y tiene por objeto, garantizar la protección de los datos personales que se encuentran en posesión de los sujetos obligados así como establecer los principios, derechos, excepciones, obligaciones, sanciones y responsabilidades que rigen en la materia.
- Que son Finalidades de la Ley:
  - Garantizar la observancia de los principios de protección de datos personales en posesión de los sujetos obligados;
  - Proveer lo necesario para que toda persona pueda ejercer los derechos de acceso, rectificación y cancelación de sus datos personales, así como manifestar su oposición a determinado tratamiento, mediante procedimientos sencillos y expeditos;
  - Promover la adopción de medidas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de los datos personales en posesión de los sujetos obligados.
- Que son sujetos obligados para la aplicación de la Ley, el Poder Ejecutivo, el Poder Legislativo; el Poder Judicial, los Ayuntamientos; los Órganos y Organismos Constitucionales Autónomos; y los Tribunales Administrativos.
- Que se entiende por **datos personales**<sup>1</sup> cualquier información concerniente a una persona física identificada o identificable.<sup>2</sup>

<sup>1</sup> Centrándonos en la definición de *datos de carácter personal*, en alcance de dicho concepto alude a dos naciones, el primero al significado de dato y su vinculación con la persona. Siendo que *por dato* debe entenderse toda aquella información que nos permite llegar al conocimiento de una cosa, bien sea directa o indirectamente. Por ende, se podría deducir con meridiana claridad que el objeto de protección del derecho fundamental a la protección de los datos no se reduce sólo a los *datos íntimos de la persona*, sino a cualquier tipo de dato o no fundamentales, porque

- Que se entiende como **derechos ARCO**, los derechos de **acceso, rectificación, cancelación y oposición** de datos personales.
- Que los **derechos ARCO** son **derechos independientes**. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro.
- Que por ello el ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio del otro.
- Que **puede dirigirse a cualquiera de los organismos públicos**, de los que sabe o presume que tienen sus datos, solicitando información sobre qué datos tienen y cómo los han obtenido y las cesiones o transmisiones que, a su vez, haya realizado (derecho de acceso), la rectificación de los mismos, o en su caso, la cancelación de los datos en sus ficheros (derecho de cancelación).
- Se debe dirigir al Sujeto Obligado en el que se encuentren los datos personales, utilizando cualquier medio que permita acreditar el envío y la recepción de la solicitud, pero asegurando la identidad o representación, acompañando copia de identificación oficial, ya sea credencial para votar, pasaporte o cualquier otra.

su objeto no es solo la intimidación individual, sino los datos de carácter personal. Por lo que hace, a *dato personal*, se considera cualquier información concerniente a un *apersona física identificada o identificable*.

<sup>2</sup> Resulta oportuno, señalar que el concepto de "*cualquier información concerniente a una persona física identificada o identificable*"; implica una definición sin calificativo, lo cual hace que sea una definición amplia y no restrictiva del concepto, lo que permite ampliar la protección sobre los datos que conciernen a la persona. Ejemplos de datos personales de un individuo: nombre, sexo, nacionalidad, firma, huella dactilar, IRIS, ADN, profesión, número personal de celular, número personal de correo electrónico, patrimonio, estado civil, números de cuenta bancaria, preferencia sexual, religión, preferencia política, color de piel, imagen, estado de salud, por citar algunos.

Al aludir a "*cualquier información*", se refiere al gran espectro de información *personal*, a toda aquella que se relacione con una persona física, llámeselos datos comunes, habituales y no habituales, fundamentales o no, íntimos o no. Y al referir a "*persona física*" es decir se protege solo a *personas humanas*, no aplicable a personas jurídicas colectivas como se expondrá más adelante, las cuales no significan que no puedan tener o contar con otro tipo de protección jurídica, pero no la relativa a la protección de datos de carácter personal.

Y finalmente "*identificada*" o "*identificable*" que significa en el primer caso que ya se sabe la identidad actual de la misma. Por su parte, se considera *identificable* toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. Siendo así un individuo no se considera *identificable* si la identificación requiere de una cantidad de tiempo y medios no razonables (complejo, caros, extraordinarios, etc.). Por lo que si los medios no son razonables la persona ya no se considera *identificable* y los datos tendrán el carácter de anónimos.

Y solo como corolario, cabe decir que la definición de dato de carácter personal es esencial, pues constituye el ámbito de aplicación objetivo de la normativa, es decir, en caso de que consideráramos que algo no es dato de carácter personal, la normativa no se aplicaría, por lo que resulta exigente una definición amplia y correcta con el fin de que la protección sea la más adecuada.

- Que los sujetos obligados están obligados a orientar en forma sencilla y comprensible a toda persona sobre los trámites y procedimientos que deben efectuarse para ejercer los derechos ARCO, las autoridades o instancias competentes, la forma de realizarlos, la manera de llenar los formularios que se requieran, así como de las instancias ante las que se puede acudir a solicitar orientación o formular quejas, consultas o reclamos sobre la prestación del servicio o sobre el ejercicio de las funciones o competencias a cargo de los servidores públicos de que se trate.
- Que el ejercicio de los mismos es personalísimo, y debe, por tanto, ser ejercido directamente por los interesados ante cada uno de los responsables. Por eso se plantea prever que sin perjuicio de lo que dispongan otras leyes, solo los titulares o sus representantes legales podrán solicitar a través de la Unidad de Información, previa acreditación, en términos de lo que establezca las disposiciones reglamentarias.
  - Que el titular de los datos podrá denunciar ante el Instituto por posibles violaciones a las disposiciones establecidas en esta Ley, a fin de que se proceda a realizar la investigación respectiva y en su momento a emitir la resolución que en derecho proceda.
  - Que en caso de que el Instituto tenga conocimiento, por cualquier otro medio de posibles violaciones a las disposiciones de la Ley o los lineamientos, podrá iniciar de oficio la investigación respectiva.
- Que los sujetos obligados deberán adoptar, mantener y documentar las medidas de seguridad administrativa, física y técnica necesarias para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, mediante acciones que eviten su daño, alteración, pérdida, destrucción, o el uso, transmisión y acceso no autorizado, de conformidad con lo dispuesto en los lineamientos que al efecto se expidan.
- Que dichas medidas serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales, deberán constar por escrito y ser comunicadas al Instituto para su registro.
- Que las medidas de seguridad que al efecto se establezcan deberán indicar el nombre y cargo del servidor público responsable o, en su caso, la persona física o

jurídica colectiva que intervengan en el tratamiento de datos personales con el carácter de responsable del sistema de datos personales o usuario, según corresponda. Cuando se trate de usuarios se deberán incluir los datos del acto jurídico mediante el cual, el sujeto obligado otorgó el tratamiento del sistema de datos personales.

- Que el sujeto obligado responsable de la tutela y tratamiento del sistema de datos personales, adoptando medidas de seguridad,

Es así, que la Ley de Protección de Datos Personales del Estado de México y Municipios, tiene por objeto, garantizar la protección de los datos personales que se encuentran en posesión de los sujetos obligados de esta entidad federativa, ello mediante la observancia a los principios, derechos, excepciones, obligaciones, sanciones y responsabilidades que rigen en la materia. Es decir, la presente Ley viene a regular el derecho fundamental reconocido en el segundo párrafo al artículo 16 de la Constitución Federal que reconoce la existencia de un nuevo derecho distinto y fundamental a la protección de datos personales, dentro del catálogo de garantías.

Cabe recordarse que dicho derecho se dio en razón de la evolución normativa experimentada en nuestro país, a partir de la regulación de la protección de datos personales en posesión del Estado regulada por la fracción II del artículo 6o. constitucional. La intención de reformar el artículo 16 para incluir la protección de los datos personales, fue un camino que desde hace algún tiempo inició el legislador mexicano.

Precisado lo anterior se tiene que **EL RECURRENTE** refiere dentro de sus motivos de inconformidad que "SOLICITO QUE EL PRESENTE RECURSO DE REVISIÓN SE ENDERECE COMO DENUNCIA TODA VEZ QUE LA RESPUESTA CONTENIDA EN EL ARCHIVO EN COMENTO VIOLA EN TODOS SENTIDOS LO DISPUESTO EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO" (sic)

Por lo anterior este Instituto advierte que sin duda utiliza el formato de "recurso de revisión" y utiliza **EL SAIMEX** para hacer de conocimiento tanto de **EL SUJETO OBLIGADO** como de este Órgano Garante la publicación de Datos Personales. Con lo anterior, lo que se pretende señalar es que, en principio y a primera vista pareciera que no se está ante un "recurso de revisión", más aún que **EL SAIMEX** es el del Sistema de Acceso a la Información Mexiquense.

Debe tomarse como punto de partida la máxima ya establecida de se debe garantizar la protección de los datos personales que se encuentran en posesión de los sujetos obligados de esta entidad federativa, ello mediante la observancia a los principios, derechos, excepciones, obligaciones, sanciones y responsabilidades que rigen en la materia Ley de Protección de Datos Personales del Estado de México y Municipio.

Si se atiende con más detenimiento en el texto de los motivos de inconformidad, se observa que refiere a la siguiente acción que debe realizar **EL SUJETO OBLIGADO**: *garantizar la protección de los datos personales que se encuentran en posesión de los sujetos obligados.*

Pero entonces, vale cuestionar ¿por qué EL RECURRENTE utilizó EL SAIMEX para hacer del conocimiento el incumplimiento de los deberes legales de los Sujetos Obligados sobre el ejercicio de los derechos ARCO?

Por la sencilla razón de que es el único mecanismo institucional de naturaleza electrónica que permite poner en contacto a los solicitantes, a los Sujetos y a este Órgano Garante. O bien, dicho en sentido negativo, porque no hay otro sistema electrónico que permita poner en conocimiento del Instituto el incumplimiento de dichos deberes legales de los Sujetos Obligados.

En efecto a través del recurso de revisión el RECURRENTE se inconforma porque LA RESPUESTA CONTENIDA EN EL ARCHIVO EN COMENTO VIOLA EN TODOS SENTIDOS LO DISPUESTO EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO y por donde se quiera ver eso es una denuncia sobre la publicación de datos personales.

Es claro que el hecho de que LA RESPUESTA CONTENIDA EN EL ARCHIVO EN COMENTO VIOLA EN TODOS SENTIDOS LO DISPUESTO EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO, sin prejuzgar los alcances de la publicación pudiesen representar un incumplimiento sobre garantizar la protección de los datos personales lo que se hace valer mediante un recurso de revisión.

El recurso de revisión está destinado a impugnar el incumplimiento de los Sujetos Obligados en torno a solicitudes de acceso a información o bien de solicitudes de acceso a datos personales según sea el caso, pero no para inconformarse con todo tipo de incumplimiento a la Ley de Transparencia o de la Ley Protección de Datos personales. Sería tanto como afirmar que el recurso de revisión es el único mecanismo para

EXPEDIENTE: 01027/INFOEM/IP/RR/2014  
SUJETO OBLIGADO: AYUNTAMIENTO DE TENANGO DEL VALLE  
COMISIONADA PONENTE: EVA ABAID YAPUR

VOTO EN CONTRA DE: FEDERICO GUZMÁN TAMAYO.

inconformarse y dejar de lado otras vías, como por ejemplo, la exigencia de responsabilidades administrativas, la vista al Ministerio Público, entre otros.

Y lo razonado en los párrafos anteriores no sólo tiene una lógica irrefutable, sino un reconocimiento jurídico en el marco de las atribuciones del Instituto. Así, mientras que la atribución esencial de este órgano Garante es la resolución de los recursos de revisión, conforme a la fracción III del artículo 66 de la Ley de Protección de Datos Personales del Estado de México y Municipios, cuenta con otras atribuciones que el mismo precepto le señala:

*Título Séptimo  
Del Instituto de Transparencia, Acceso a la Información Pública y Protección de  
Datos  
Personales del Estado de México y Municipios*

*Capítulo Tercero  
Del Instituto*

*Del Órgano Garante*

*Artículo 65.- El Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, es la autoridad encargada de garantizar a toda persona la protección de sus datos personales que se encuentren en posesión de los sujetos obligados, a través de la aplicación de la presente Ley.*

*Atribuciones del Órgano Garante*

*Artículo 66. El Instituto en la materia, tendrá las siguientes atribuciones:*

- I. Interpretar en el orden administrativo la presente Ley;*
- II. Orientar y asesorar a los particulares acerca de las solicitudes materia de esta Ley;*
- III. Conocer y resolver los recursos de revisión interpuestos por los solicitantes;*
- IV. Establecer políticas y lineamientos para el manejo, tratamiento, seguridad y protección de los datos personales en posesión de los sujetos obligados;*
- V. Diseñar y aprobar los formatos de solicitudes de acceso, rectificación, cancelación y oposición de datos personales;*
- VI. Llevar a cabo el Registro de los sistemas de datos personales en posesión de los sujetos obligados;*
- VII. Elaborar y actualizar el registro del nivel de seguridad aplicable a los sistemas de datos personales en posesión de las dependencias y entidades; así como establecer los estándares mínimos que deberán contener los documentos de seguridad de los sujetos obligados;*
- VIII. Formular observaciones y recomendaciones a los sujetos obligados que incumplan esta Ley.*
- IX. Proporcionar apoyo técnico a los sujetos obligados en materia de protección de datos personales, así como celebrar con ellos, convenios de colaboración orientados a apoyar la capacitación de los servidores públicos responsables de los sistemas de datos personales;*

X. Proporcionar a los sujetos obligados un sitio web tipo el cual deberá contener cuando menos información pública de oficio, así como cualquier otra información que considere conveniente difundir en materia de protección de datos personales;

XI. Elaborar la Guía de Procedimientos a que hace referencia esta Ley;

XII. Llevar a cabo las Manifestaciones de Impacto a la Privacidad a petición de los sujetos obligados;

XIII. Capacitar a los servidores públicos en materia de protección de datos personales;

XIV. Llevar a cabo visitas de verificación en materia de seguridad de sistemas de datos personales en posesión de los sujetos obligados;

XV. Investigar las posibles violaciones a las disposiciones de esta Ley a que hace referencia el artículo 32 de esta Ley;

XVI. Hacer del conocimiento del órgano interno de control del sujeto obligado que corresponda, las presuntas infracciones a esta Ley así como a sus lineamientos expedidos en la materia;

XVII. Procurar la conciliación entre las autoridades y los titulares de los datos personales en cualquier momento del procedimiento, y en su caso, verificar el cumplimiento del acuerdo respectivo;

XVIII. Incluir en el informe anual de actividades que está obligado a presentar ante el Poder Legislativo del Estado de México, en términos de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, un informe detallado en materia de protección de datos personales, que incluya la información a que hace referencia el artículo 69;

XIX. Promover entre las instituciones educativas públicas y privadas la difusión de la cultura de protección de datos personales;

XX. Elaborar y publicar estudios e investigaciones; así como organizar seminarios, cursos, talleres y demás actividades que permitan difundir y ampliar el conocimiento sobre la materia de esta Ley;

XXI. Emitir lineamientos y criterios en materia de protección de datos personales;

XXII. Establecer procedimientos para verificar el cumplimiento de la ley, por parte de los sujetos obligados; e

XXIII. Implementar los procedimientos e imponer las sanciones previstas en la ley, con base en la Ley de Responsabilidades de los Servidores Públicos del estado y Municipios.

Del citado precepto cabe destacar para el caso que nos ocupa lo siguiente:

- ✓ La facultad de interpretar administrativamente la Ley de protección de datos personales.
- ✓ La atribución genérica para vigilar a los Sujetos Obligados en el cumplimiento de la Ley de la materia, diferente a la facultad para resolver los recursos de revisión.
- ✓ La de establecer los procedimientos para que los Sujetos Obligados cumplan con la Ley de la materia.
- ✓ Establecer lineamientos y criterios de carácter obligatorio respecto a datos personales, corrección o supresión de éstos para todos los Sujetos Obligados de la Ley.
- ✓ De apoyar a los Sujetos Obligados en el cumplimiento de las obligaciones que les impone la presente Ley.

- ✓ De hacer del conocimiento del órgano de control interno o equivalente de cada Sujeto Obligado las infracciones a esta Ley.
- ✓ Formular observaciones y recomendaciones a los sujetos obligados que incumplan esta Ley.
- ✓ De establecer procedimientos para verificar las acciones realizadas por los Sujetos Obligados en el cumplimiento de sus obligaciones en términos de la presente Ley;

Visto así, la conclusión a la que conlleva la argumentación anterior es que el expediente número 01027/INFOEM/IP/RR/2014 no es en rigor, a pesar de las formalidades, un recurso de revisión, sino que en términos de Derecho Administrativo cuando particular expone el incumplimiento de una autoridad a una obligación legal dicha exigencia se le denomina "denuncia".

Más aún, si el Instituto se erige en una especie de órgano fiscalizador independiente al papel de órgano resolutor, para que los Sujetos Obligados cumplan con lo que la Ley de Transparencia establece. Y el señalamiento que un particular hace ante un incumplimiento, en el fondo se trata de una denuncia hecha ante este Órgano Garante, misma que debió ser analizada por el órgano Competente y en su caso determinar su viabilidad o no de la misma.

En consecuencia, se considera que era procedente ordenar el enderezamiento o encausamiento de este recurso de revisión como denuncia.

Debe señalarse que el enderezamiento de un recurso por la correcta naturaleza del pedimento cuenta con diversos precedentes por analogía en caso de denuncia de incumplimiento de IPO del Expediente Complementario de Incidente de Denuncia o Queja No. 01875/ITAIPEM/IP/RR/A/2009 proyectado por la Ponencia del Comisionado Federico Guzmán Tamayo y aprobado por mayoría de votos en la sesión ordinaria del 29 de septiembre de 2009, así como el caso del Expediente 00086/INFOEM/IP/RR/A/2010 proyectado también por esa misma Ponencia y que fuera aprobado por mayoría de votos en la sesión ordinaria de fecha 10 de marzo del año en curso. Los precedentes antes enunciados se invocan solo para dejar claro que la Ponencia del suscripto ya se ha pronunciado en otras ocasiones para enderezar o encauzar los procedimientos y darles el tratamiento que a su naturaleza corresponda.

En abundamiento, a la justificación para el enderezamiento o encausamiento de este recurso de revisión como denuncia, resulta como elementos de juicio para ello lo siguiente:

EXPEDIENTE: 01027/INFOEM/IP/RR/2014  
**SUJETO OBLIGADO:** AYUNTAMIENTO DE TENANGO DEL VALLE  
**COMISIONADA PONENTE:** EVA ABAID YAPUR  
**VOTO EN CONTRA DE:** FEDERICO GUZMÁN TAMAYO.

### **Derecho del Titular a Presentar Denuncias**

*Artículo 32.- El titular de los datos podrá denunciar ante el Instituto por posibles violaciones a las disposiciones establecidas en esta Ley, a fin de que se proceda a realizar la investigación respectiva y en su momento a emitir la resolución que en derecho proceda.*

*Asimismo, en caso de que el Instituto tenga conocimiento, por cualquier otro medio, de posibles violaciones a las disposiciones de la Ley o los lineamientos, podrá iniciar de oficio la investigación respectiva.*

*Las denuncias serán tramitadas en términos del procedimiento aprobado por el Instituto.*

*Cuando derivado de la investigación de los casos de violación del derecho a la protección de datos personales, se desprenda que puede existir menoscabo de otros derechos humanos correlativos, el Instituto se coordinará con las instancias u organismos competentes, para la investigación correspondiente, con la finalidad de garantizar cabalmente la protección integral de dichos derechos humanos.*

### **LINEAMIENTOS SOBRE MEDIDAS DE SEGURIDAD APLICABLES A LOS SISTEMAS DE DATOS PERSONALES QUE SE ENCUENTRAN EN POSESIÓN DE LOS SUJETOS OBLIGADOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO:**

#### *Capítulo Segundo*

#### *De la denuncia por violación a las disposiciones de la Ley*

##### *De la denuncia del titular de los datos personales*

*Artículo 87. En términos del artículo 32 de la Ley, el titular de los datos personales podrá presentar denuncias ante el Instituto, por posibles violaciones a las disposiciones establecidas en la misma Ley.*

*Al presentarse una denuncia, el Instituto deberá instaurar y desarrollar el procedimiento de verificación que se establece en estos Lineamientos, así como emitir la resolución que en derecho proceda.*

### **LINEAMIENTOS POR LOS QUE SE ESTABLECEN LAS POLÍTICAS, CRITERIOS Y PROCEDIMIENTOS QUE DEBERÁN OBSERVAR LOS SUJETOS OBLIGADOS, PARA PROVEER LA APLICACIÓN E IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO:**

EXPEDIENTE: 01027/INFOEM/IP/RR/2014

SUJETO OBLIGADO: AYUNTAMIENTO DE TENANGO DEL  
VALLE

COMISIONADA PONENTE: EVA ABAID YAPUR

VOTO EN CONTRA DE: FEDERICO GUZMÁN TAMAYO.

## TÍTULO SEXTO

### *De la denuncia por violación a las disposiciones de la Ley*

#### *Capítulo Único*

### *De la denuncia por violación a las disposiciones de la Ley*

#### *De la denuncia del titular de los datos personales*

*Artículo 103. En términos del artículo 32 de la Ley, el titular de los datos personales podrá presentar denuncias ante el Instituto por posibles violaciones a las disposiciones establecidas en la misma Ley.*

*Cuando se presenta una denuncia, el Instituto deberá instaurar y desarrollar el procedimiento de verificación correspondiente y emitir la resolución que en derecho proceda.*

#### *De los requisitos de la denuncia*

##### *Artículo 104. La denuncia deberá indicar lo siguiente:*

*I. Nombre del denunciante y domicilio o medio para recibir notificaciones, en su caso;*

*II. Sujeto Obligado denunciado, y*

*III. Relación de los hechos en los que basa su denuncia y los elementos con los que cuente para probar su dicho.*

*La denuncia podrá presentarse por escrito ante el Instituto o por correo electrónico institucional.*

*Cuando la denuncia se presente por medios electrónicos, se entenderá que se acepta que las notificaciones sean efectuadas a través de dicho sistema.*

*Cuando las actuaciones se lleven a cabo como consecuencia de una denuncia, el Instituto acusará recibo de ésta, pudiendo solicitar la documentación que estime oportuna para el desarrollo del procedimiento.*

Todo lo anterior, sin duda permite al Suscrito refrendar la justificación para desglosar el encauzamiento de la denuncia implícita que se deriva de la propia manifestación del ahora RECURRENTE. Lo que conllevaba refrendar la justificación para dar vista al Órgano de Control Interno y Vigilancia de los hechos que se denuncian respecto del incumplimiento a la Ley de Protección de Datos Personales en el Estado de México y Municipios.

Sin embargo, respecto de esto resulta oportuno definir el procedimiento a seguir cuando se ha concluido que se trata de una denuncia de incumplimiento de la Información de Oficio.

Como ya se observó, el Instituto tiene en conjunto las siguientes atribuciones:

#### **Atribuciones del Órgano Garante**

*Artículo 66.- El Instituto en la materia, tendrá las siguientes atribuciones:*

*I. Interpretar en el orden administrativo la presente Ley;*

*XXII. Establecer procedimientos para verificar el cumplimiento de la ley, por parte de los*

Instituto de Transparencia, Acceso a la Información Pública y  
Protección de Datos Personales del Estado de México y Municipios

Instituto Literario Pte. No. 510,  
Col. Centro, C.P. 50000, Toluca, México.  
Tels. (722) 2 2 6 19 80,  
Lado sin costo: 01 800 821 0441

[www.Infoem.org.mx](http://www.Infoem.org.mx)

*XXIII. Implementar los procedimientos e imponer las sanciones previstas en la ley, con base en la Ley de Responsabilidades de los Servidores Públicos del estado y Municipios*

En vista de ello, no hay procedimiento establecido en una regulación *ad hoc*, lo que determina que el propio Instituto mediante Resolución deba definir tal procedimiento para el caso concreto.

Luego entonces, los elementos básicos a definir como procedimiento para la denuncia son los siguientes:

- Instancia ante la que se desahoga o da seguimiento a la denuncia.
- Plazos de cumplimiento.

En lo tocante a la instancia ante la que se desahoga la denuncia, si bien el Pleno es el órgano máximo del Instituto, también lo es que la esencia del mismo es la de un órgano resolutor de recursos de revisión, que no de denuncias. Y aunque el Instituto tiene la atribución de vigilar dichos cumplimientos, no necesariamente lo hará a través del Pleno, si para ello cuenta con el Órgano de Control Interno y Vigilancia.

En virtud de lo anterior, la instancia del Instituto responsable de desahogar el procedimiento o en su caso seguimiento de denuncia de incumplimiento de posibles violaciones en materia de protección de datos es el Órgano de Control y Vigilancia, a la cual se debió turnar para los efectos a la denuncia a efecto de dar seguimiento al cumplimiento de la resolución, seguimiento que entre otros aspectos comprendería el de revisar en principio la procedencia o improcedencia de la Denuncia, por lo que de determinarse procedente la misma y de estimarse una violación a la Ley de Protección de Datos Personales del Estado de México se procedería a incoar el procedimiento de responsabilidad administrativa en contra de los servidores públicos respectivos que en su caso resultaran responsables, ello en términos del Título Séptimo de la Ley de Protección de Datos Personales en el Estado de México y Municipios. En todo caso debería informar al Pleno en su momento procesal oportuno sobre el seguimiento de la denuncia y cumplimiento de lo en su momento resuelto.

Por las razones anteriores el suscripto considera que lo procedente era enderezar el recurso de revisión interpuesto como denuncia en términos de lo expuesto, con fundamento en las fracciones I, XXII del artículo 66 de la Ley de Protección de Datos Personales en el Estado de México y Municipios.

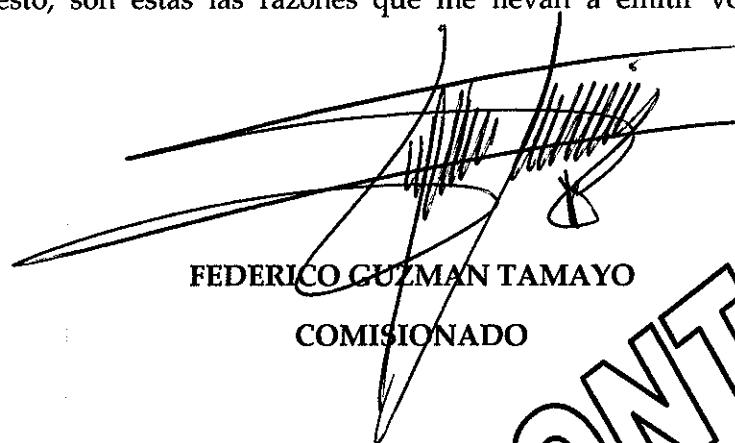
Y en consecuencia turnar la denuncia (enderezada) al Órgano de Control y Vigilancia de este Instituto como área competente para el seguimiento respectivo de la denuncia y para la

EXPEDIENTE: 01027/INFOEM/IP/RR/2014  
SUJETO OBLIGADO: AYUNTAMIENTO DE TENANGO DEL  
VALLE  
COMISIONADA PONENTE: EVA ABAID YAPUR

VOTO EN CONTRA DE: FEDERICO GUZMÁN TAMAYO.

verificación del debido cumplimiento por lo que hace a la denuncia sobre la publicidad de datos personales del **SUJETO OBLIGADO**.

Por lo expuesto, son estas las razones que me llevan a emitir voto en contra de la resolución.

  
FEDERICO GUZMAN TAMAYO  
COMISIONADO

VOTO EN CONTRA