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

Metepec, Estado de México, 17 de julio de 2015
Oficio No. INFOEM/COM-JMC/099/2015

Mtra. CATALINA CAMARILLO ROSAS
SECRETARIO TECNICO DEL PLENO
PRESENTE

Por instrucción del comisionado Mtro. Javier Martínez Cruz y con fundamento en los artículos 20, fracciones I y IV; 30 fracción X y 43, fracciones I, II, XIII y XVI del Reglamento Interior del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, adjunto al presente se servirá encontrar original del voto disidente, emitido por el comisionado en cita, en la resolución del recurso de revisión 00919/INFOEM/IP/RR/2015, aprobada en el pleno de este instituto, en la vigésima quinta sesión ordinaria de fecha siete de julio de dos mil quince.

ATENTAMENTE

COORDINADORA DE PROYECTOS

NORMA ARANSASU VALDES PEDRAZA

A
Infoem
03 Ago 2015
RECIBIDO
OFI. SA
COM. EAY
3:01 pm

C.c.p. **Dra. Josefina Román Vergara.** Comisionada.
Mtra. Eva Abaid Yapur. Comisionada.
Mtra. Zulema Martínez Sánchez. Comisionada.
Mtro. Javier Martínez Cruz. Comisionado.
Para conocimiento y efectos legales conforme al artículo 20, fracción I del Reglamento Interior del Instituto de Transparencia, Acceso a la Información Pública y protección de Datos Personales del Estado de México y Municipios.

Metepec, Estado de México, 15 de julio de 2015

VOTO DISIDENTE QUE FORMULA EL COMISIONADO JAVIER MARTÍNEZ CRUZ RELATIVO AL RECURSO DE REVISIÓN 00919/INFOEM/IP/RR/2015.

En la sesión de fecha siete de julio de dos mil quince correspondiente a la vigésima quinta sesión ordinaria, el Pleno del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México resolvió por mayoría de votos, el recurso de revisión **00919/INFOEM/IP/RR/2015** presentado por la Comisionada Eva Abaid Yapur, resolución que es materia del presente **VOTO DISIDENTE** que el suscrito formula con fundamento en las fracciones I y IV del artículo 20 y 30, fracción X del Reglamento Interior del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios.

El suscrito no comparte el estudio y sentido de la resolución pronunciada, cuyo resolutivo ordenó entregar "La Plantilla del personal sindicalizado perteneciente al ODAPAS, en la que se contenga el nombre de dicho personal sindicalizado", toda vez que la mayoría analizó las razones o motivos de inconformidad debatidos por la recurrente y fundamentó el estudio de la resolución esencialmente en lo dispuesto por los artículos 2, fracciones V y XV; 3 y 11 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, que ordenan:

*"**Artículo 2.**- Para los efectos de esta Ley, se entenderá por:*

V. Información Pública: La contenida en los documentos que los sujetos obligados ***generen en el ejercicio de sus atribuciones;***

XV. Documentos: Los expedientes, estudios, actas, resoluciones, oficios, acuerdos, circulares, contratos, convenios, estadísticas o bien cualquier registro en posesión de los sujetos obligados, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en medios escritos, impresos, sonoros, visuales, electrónicos, informáticos u holográficos; y"

Artículo 3.- *La información pública generada, administrada o en posesión de los Sujetos Obligados* ***en ejercicio de sus atribuciones****, será accesible de manera permanente a cualquier persona, privilegiando el principio de máxima publicidad de la información. Los Sujetos Obligados deben poner en práctica, políticas y programas de acceso a la información que se apeguen a criterios de publicidad, veracidad, oportunidad, precisión y suficiencia en beneficio de los solicitantes.*

Artículo 11.- *Los Sujetos Obligados sólo proporcionarán la información que* ***generen en el ejercicio de sus atribuciones.****"*

De lo anterior se aprecia que la materia esencial del recurso de revisión está relacionada con la filiación sindical de los servidores públicos involucrados, por lo que a consideración de esta ponencia, la resolución que se analiza transgredió el derecho a la protección de datos personales en posesión del sujeto obligado, tutelado por la Ley de Protección de Datos Personales del Estado de México y en agravio de cada servidor público listado.

Ya que en el SEGUNDO resolutivo, al ordenar que se entregue el o los documentos en los que conste la plantilla del personal sindicalizado perteneciente al ODAPAS, tiene como consecuencia que el SUJETO OBLIGADO genere un documento *ad hoc,*

al nivel de detalle solicitado para satisfacer el requerimiento de la RECURRENTE, ante lo cual, lo pertinente era ordenar la entrega de la NÓMINA, que en el presente caso sí genera el SUJETO OBLIGADO, por lo que a consideración de esta ponencia, con lo resuelto se transgrede lo dispuesto en el artículo 41 de la Ley de Transparencia y Acceso a la Información de la entidad que ordena:

> *"**Artículo 41.-** Los Sujetos Obligados sólo proporcionarán la información pública que se les requiera y que obre en sus archivos. No estarán obligados a procesarla, resumirla, efectuar cálculos o practicar investigaciones."*

Lo expuesto también tiene sustento en consideración de que la afiliación sindical es un dato personal sensible que puede afectar la intimidad de su titular; más aún, su utilización indebida puede dar origen a alguna forma de discriminación en contra de las personas simpatizantes de cierta ideología sindical, por lo que su publicación inminentemente puede producir un daño mayor que el interés público de conocer la información solicitada por algún particular, lo cual se fundamenta en los "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" que en sus artículos 1, fracciones I y VIII; 7 y 8 ordenan:

> *"**Artículo 1.** Los datos personales contenidos en los sistemas de datos personales se clasificarán, de manera enunciativa y no limitativa, en las siguientes categorías:*
>
> ***I. Datos de identificación**: Nombre; domicilio; teléfono particular y/o celular; correo electrónico personal; estado civil; firma; firma electrónica;*

cartilla militar; lugar y fecha de nacimiento; nacionalidad; edad; fotografía; clave del Registro Federal de Contribuyentes (RFC); Clave Única de Registro de Población (CURP); nombres de familiares, dependientes y beneficiarios; costumbres; idioma o lengua, y voz, entre otros;

II. a VII. (…)

***VIII. Datos ideológicos**: Creencias religiosas; ideología; **afiliación política y/o sindical**, y pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros;*

IX. a XII. (…)"

*"**Artículo 7.** En términos del artículo 59, inciso B, de la Ley, las medidas de seguridad se clasificarán en tres niveles: básico, medio y alto.*

Dichas medidas serán acumulativas; es decir, el nivel medio comprenderá las medidas del nivel básico, mientras que el nivel alto incluirá tanto las medidas del nivel básico como del nivel medio.

***Artículo 8.** Las medidas de seguridad aplicables a los sistemas de datos personales responderán a los niveles señalados en la Ley para cada categoría de datos personales. Dichas medidas deberán tomar en consideración las recomendaciones que, en su caso, emita el Instituto para este fin, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales durante su tratamiento.*

En todo caso, deberán tomarse en cuenta los criterios internacionales establecidos en la materia, sobre medidas de seguridad para el resguardo eficaz de los datos personales.

Al final de cada medida sugerida, se establecen los niveles de seguridad que habrán de observarse, según la naturaleza de la información contenida en los sistemas de datos personales.

Los niveles de seguridad deberán responder a la mayor o menor necesidad de garantizar la integridad de los datos personales.

Los Sujetos Obligados aplicarán el nivel básico, medio o alto de acuerdo con las categorías de datos personales indicadas a continuación:

***I. Nivel básico**: Estas medidas de seguridad serán aplicables a todos los sistemas de datos personales.*

En los sistemas de datos personales que contengan alguna de las categorías de datos que se enlistan a continuación, resultarán aplicables, al menos, las medidas de seguridad de nivel básico:

a) Datos de identificación, y

b) Datos laborales;

***II. Nivel medio:** En los sistemas de datos personales que contengan alguna de las categorías de datos que aparecen a continuación, resultarán aplicables tanto las medidas de seguridad de nivel básico como las de nivel medio:*

a) Datos patrimoniales,

b) Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales,

c) Datos académicos, y

d) Datos de tránsito y movimientos migratorios, y

***III. Nivel alto**: En los sistemas de datos personales que contengan alguna de las categorías de datos que aparecen a continuación, resultarán aplicables tanto las medidas de seguridad de nivel básico y medio como las de nivel alto:*

a) Datos de salud;

b) Datos ideológicos;

c) Datos de origen;

d) Datos biométricos dinámicos y/o estáticos, y

e) Datos de vida sexual."

Al respecto y toda vez que éste órgano Garante 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 Ley de Protección de Datos Personales del Estado de México, se concluye que los datos personales ideológicos como lo son la afiliación sindical, se consideran datos personales que encuadran en un nivel alto de seguridad y en consecuencia en el caso concreto debió aplicarse lo previsto en los artículos 59 inciso B fracción III y 60 de la Ley de Protección de Datos Personales del Estado de México que prevén:

> *"**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. (...)*
>
> *B. **Niveles de seguridad**:*
>
> *I., II. (...)*
>
> ***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.*

> ***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."*

Consecuentemente, el sujeto obligado al no adoptar las medidas conducentes y más aún, con la resolución determinada, se transgrede lo dispuesto en los artículos 4 fracción VIII, 8, 17, 33 y 58 párrafo primero de la Ley de Protección de Datos Personales de la entidad, en perjuicio de los servidores públicos listados, vulnerando con ello su derecho a la protección de datos personales, toda vez que los numerales citados disponen:

> ***Artículo 4.-*** *Para los efectos de esta Ley se entiende por:*
>
> *I a VII.*
>
> *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;*
>
> ***Artículo 8.-*** *Todo tratamiento de datos personales en posesión de los sujetos obligados deberá contar con el consentimiento de su titular.*
>
> *El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos en los términos previstos en la ley. Para*

revocar el consentimiento, el responsable deberá realizar la indicación respectiva en el aviso de privacidad.

***Artículo** 17.- Los datos personales sensibles son irrenunciables, intransferibles e indelegables, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del titular.*

Dicha obligación subsistirá aún después de finalizada la relación entre el sujeto obligado con el titular de los datos personales, así como después de finalizada la relación laboral entre el sujeto obligado y el responsable del sistema de datos personales o los usuarios.

***Artículo** 33.- Cuando los datos personales sensibles sean objeto de tratamiento, el sujeto obligado deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa o cualquier mecanismo de autenticación.*

Sólo podrán crearse sistemas de datos personales sensibles, cuando así lo disponga la ley, mismos que deberán ser debidamente resguardados; garantizándose el manejo cuidadoso de los mismos.

El responsable del sistema de datos personales o en su caso los usuarios autorizados son los únicos que puedan llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan.

Los responsables y encargados que intervengan en cualquier fase del tratamiento de datos deberán guardar confidencialidad respecto de estos; obligación que subsistirá mientras permanezca en el cargo, empleo o comisión, e incluso cinco años después de finalizar sus relaciones con el sujeto obligado, salvo disposición legal en contrario.

***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."

Ahora bien, el artículo 7 de la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, establece como deber de los sujetos obligados de hacer pública toda la información respecto a los montos y personas a quienes se entreguen recursos públicos, pero también el Artículo 25 del mismo ordenamiento, establece que se considera información confidencial de acuerdo a su fracción I, cuando contenga datos personales, entendiendo por estos conforme al artículo 2 de la Ley en comento, la información concerniente a una persona física, identificada o identificable.

Finalmente cabe señalar que por tratarse de datos personales clasificados como ideológicos con nivel de seguridad alto por referirse a filiación sindical, debe

anteponerse la protección de los datos de referencia ante el derecho de acceso a la información pública, tal y como lo ha sostenido este Instituto garante en diversas resoluciones que fungen como antecedente de este criterio, por lo que ésta Ponencia considera que la protección a la identidad de las personas afiliadas a algún sindicato debe prevalecer, y es el caso en que derivado del estudio en la resolución que nos ocupa, no existió pronunciamiento alguno respecto de tal situación, por lo que el resolutivo que ordena la entrega de los documentos en los que conste "la plantilla del personal perteneciente al ODAPAS, en la que contenga el nombre de dicho personal sindicalizado" vulnera la garantía a la protección de datos personales de los servidores públicos involucrados, en los términos analizados, motivos por los cuales el suscrito emite el presente voto disidente.

Javier Martínez Cruz

Comisionado