

**VOTO PARTICULAR**

Oficio: INFOEM/COM-JMC/754/2019

Metepec, Estado de México a 9 de Diciembre de 2019

**LICENCIADO EN DERECHO**

**ALEXIS TAPIA RAMÍREZ**


**SECRETARIO TÉCNICO DEL PLENO DEL INFOEM.**

**PRESENTE**

Por instrucción del Comisionado Javier Martínez Cruz, le remito para los efectos a que haya lugar el original del **voto particular** emitido por el mismo, con fundamento en el artículo 14 fracción XI del Reglamento Interior del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, con relación a la resolución emitida en el recurso de revisión **7728/INFOEM/IP/RR/2019** aprobada por el Pleno de este Instituto en la Cuadragésima Quinta Sesión Ordinaria de fecha cuatro de diciembre de dos mil diecinueve.

Sin más por el momento, aprovecho para enviarle un cordial saludo.

**ATENTAMENTE**

  
**LIC. NORMA ARANSASU VALDÉS PEDRAZA**  
**COORDINADORA DE PROYECTOS**



C.c.p.-.Mtro. José Guadalupe Luna Hernández. Comisionado. Para su conocimiento. Y efectos legales conducentes.

Instituto de Transparencia, Acceso a la Información Pública y  
Protección de Datos Personales del Estado de México y Municipios  
Teléfono: (722) 2 26 19 80 \* Centro de atención telefónica: 01 800 821 04 41

Pino Suárez S/N, actualmente Carretera Toluca-Ixtapan No. 111,  
Col. La Michoacana, Metepec, Estado de México, C.P. 52166

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



VOTO PARTICULAR QUE FORMULA EL COMISIONADO JAVIER MARTÍNEZ CRUZ, EN RELACIÓN CON LA RESOLUCIÓN DICTADA POR EL PLENO DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE MÉXICO Y MUNICIPIOS, EN LA CUADRAGÉSIMA QUINTA SESIÓN ORDINARIA DEL CUATRO DE DICIEMBRE DE DOS MIL DIECINUEVE, EN EL RECURSO DE REVISIÓN 07628/INFOEM/IP/RR/2019.

Con fundamento en lo dispuesto por el artículo 14 fracción XI del Reglamento Interior del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, el Comisionado Javier Martínez Cruz, emite **VOTO PARTICULAR** respecto a la resolución dictada en el recurso de revisión número **07728/INFOEM/IP/RR/2019**, pronunciada por el Pleno de este Instituto ante el proyecto presentado por el Comisionado José Guadalupe Luna Hernández.

En términos generales comparto el sentido de la resolución pero considero necesario realizar algunas precisiones, en ese sentido vale la pena recordar en términos concretos, para el voto que nos ocupa, que el particular solicitó del Sujeto Obligado la siguiente información:

Presupuesto anual para el CPRS desde 2015, Presupuesto detallado para 2019., Sueldo neto más prestaciones de los custodios, Sueldo neto más prestaciones de la

Directora del CPRS y de los subdirectores y jefes de área, Facturas de agua del último año., Facturas de luz del último año, Costo y factura del uniforme portado por los internos, Costo y factura de las mesas y cobijas utilizadas durante los días de visita, así como diversa información referente a los internos.

Así, cabe recordar que el Sujeto Obligado brindó respuesta a la solicitud de acceso a la información el nueve de septiembre de dos mil diecinueve, adjuntando el archivo electrónico denominado **"321 SOL.pdf"**, en el cual sustancialmente se pronuncia sobre las facturas de agua, gas y energía eléctrica.

En el estudio del fondo del asunto, se advierte un análisis minucioso para determinar la existencia de la fuente obligacional, es decir, analizar si la legislación faculta al sujeto obligado para generar, administrar o poseer las documentales solicitadas. Por lo que hace al documento en el que obren los nombres de los elementos de seguridad pública adscritos a la Secretaría, la ponencia que resuelve consideró que podía entregarse la información de manera disociada para no hacer identificable al titular del dato personal, sin embargo, a consideración del suscrito, se debió atender a la anonimización, pues mediante esta técnica se garantizará una disociación definitiva e irreversible de los datos personales<sup>1</sup>, cabe mencionar que este proceso deberá realizarse tantas veces sea necesaria según la finalidad de la información anonimizada y el interesado.

---

<sup>1</sup> Orientaciones y garantías en los procedimientos de anonimización de los datos personales. Agencia Española de Protección de Datos Personales. pp. 19.

Lo anterior con la finalidad de evitar la identificación de personas y un posible atentado a su integridad física o vida, toda vez que los miembros de las instituciones policiales se encuentran en un régimen de excepción respecto de las condiciones que presentan los servidores públicos administrativos, esto obedece a que el sólo ejercicio de las funciones que tienen encomendadas lleva implícito el riesgo a su persona derivado de la naturaleza de las funciones que desempeñan, es decir, la seguridad pública de los habitantes dentro de una demarcación territorial.

El Estado deberá garantizar y respetar los derechos humanos de los servidores públicos entre ellos, el derecho a la protección de sus datos personales, es por ello que el Estado deberá anonimizar la información, de manera que el cumplimiento de esta medida implica una reducción considerable del riesgo a una reidentificación de los individuos.

Para la Agencia Española de Protección de Datos Personales, se consideran datos identificativos directos o indirectos no necesarios, los siguientes:

*nombres, fecha de nacimiento, teléfono, DNI, email, dirección postal, número de cuentas bancarias, matrículas de vehículos, identificador dispositivo móvil, número de serie, dirección IP, identificadores biométricos, fotografía o imagen, etc.*

No debe perderse de vista que los servidores públicos de los cuales se solicitó la información realizan labores tendientes a garantizar de manera directa la seguridad nacional y pública, a través de acciones preventivas y correctivas encaminadas a

combatir a la delincuencia en sus diferentes manifestaciones. Así, es pertinente señalar que en el artículo 113, fracción I de la Ley General de Transparencia y Acceso a la Información Pública, se establece que podrá clasificarse aquella información cuya difusión pueda comprometer la seguridad nacional y pública. En este orden de ideas, una de las formas en que la delincuencia puede llegar a poner en riesgo la seguridad del país es precisamente anulando, impidiendo u obstaculizando la actuación de los servidores públicos que realizan funciones de carácter operativo, mediante el conocimiento de dicha situación, por lo que permite el acceso a la información de los prestadores de servicios en áreas de seguridad nacional o pública, puede llegar a constituirse en un componente fundamental en el esfuerzo que realiza el Estado Mexicano para garantizar la seguridad del país en sus diferentes vertientes, toda vez que como se ha mencionado con antelación, al proporcionar la información solicitada por el recurrente, es posible identificar si se trata de servidores públicos operativos, circunstancia que puede poner en riesgo la vida e integridad física de los integrantes de los cuerpos policiacos, al respecto cabe hacer mención que no debe pasar desapercibido que el artículo 81, fracción III, de la Ley de Seguridad del Estado de México, establece lo siguiente:

*“Artículo 81.- Toda información para la seguridad pública generada o en poder de Instituciones de Seguridad Pública o de cualquier instancia del Sistema Estatal debe registrarse, clasificarse y tratarse de conformidad con las disposiciones aplicables. No obstante lo anterior, esta información se considerará reservada en los casos siguientes:*

...

III. La relativa a servidores públicos miembros de las instituciones de seguridad pública, cuya revelación pueda poner en riesgo su vida e integridad física con motivo de sus funciones;

Énfasis añadido

Argumento que se fortalece con lo estipulado en el criterio número 6-09, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, antes (IFAI), el cual refiere:

"Criterio 6-09

Nombres de servidores públicos dedicados a actividades en materia de seguridad, por excepción pueden considerarse información reservada. De conformidad con el artículo 7, fracciones I y III de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental el nombre de los servidores públicos es información de naturaleza pública. No obstante lo anterior, el mismo precepto establece la posibilidad de que existan excepciones a las obligaciones ahí establecidas cuando la información actualice algunos de los supuestos de reserva o confidencialidad previstos en los artículos 13, 14 y 18 de la citada ley. En este sentido, se debe señalar que existen funciones a cargo de servidores públicos, tendientes a garantizar de manera directa la seguridad nacional y pública, a través de acciones preventivas y correctivas encaminadas a combatir a la delincuencia en sus diferentes manifestaciones. Así, es pertinente señalar que en el artículo 13, fracción I de la ley de referencia se establece que podrá clasificarse aquella información cuya difusión pueda comprometer la seguridad nacional y pública. En este orden de ideas, una de las formas en que la delincuencia puede llegar a poner en riesgo la seguridad del país es precisamente anulando, impidiendo u obstaculizando la actuación de los servidores públicos que realizan funciones de carácter operativo, mediante el conocimiento de dicha situación, por lo que la reserva de la relación de los nombres y las funciones que desempeñan los servidores públicos que prestan sus servicios en áreas de seguridad nacional o pública, puede llegar

*a constituirse en un componente fundamental en el esfuerzo que realiza el Estado Mexicano para garantizar la seguridad del país en sus diferentes vertientes” (Sic)  
Énfasis añadido.*

Sin embargo, debe tenerse en cuenta que tanto la Ley de Seguridad como el criterio orientador fueron emitidos de manera previa a la emisión de la Ley Protección de Datos Personales vigente en la Entidad, la cual fue publicada en el periódico oficial “Gaceta de Gobierno” el treinta de mayo de dos mil diecisiete, surtiendo efectos al día siguiente, en donde se incluyen los términos **disociación, anonimización, seudonimización y cifrado de datos personales**, que no son otra cosa que medidas técnicas y administrativas que evitan la asociación del titular de los datos personales con éstos, según se lee enseguida:

*“Artículo 4. Para los efectos de esta Ley se entenderá por:*

*(...)*

*II. **Anonimización:** al tratamiento que permite evitar la identificación de la o el titular a través de sus datos personales.*

*(...)*

*XVI. **Disociación:** al procedimiento por el que los datos personales no pueden asociarse a la o el titular, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo.*

*XLII. **Seudonimización:** al tratamiento de datos personales que no puedan atribuirse a un titular sin utilizar información adicional, cuando la información adicional figure por separado sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.*

*(...)*

L. *Tratamiento: a las operaciones efectuadas por los procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales...*

**Artículo 44.** *El responsable adoptará las medidas de seguridad, conforme a lo siguiente:*

(...)

IV. *De cifrado: a la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la seguridad de la información...*

**Artículo 21.** *El responsable no estará obligado a recabar el consentimiento de la o el titular para el tratamiento de sus datos personales en los casos siguientes:*

(...)

IX. *Los datos personales se sometan de manera previa a procedimientos de anonimización, disociación o seudonimización, tendientes a evitar la asociación de los datos personales con su titular....*

**Artículo 39.** *En el tratamiento aplicarán medidas técnicas y administrativas apropiadas, así como observar deberes para garantizar un nivel de seguridad adecuado al riesgo, tales como:*

(...)

II. *La disociación, anonimización y el cifrado de datos personales..."*

Así, en términos de los preceptos legales en cita, desde mi punto de vista la técnica de disociación responde a un tratamiento de datos personales efectuada mediante procedimientos manuales o automatizados que buscan la separación de la información pero aún es posible una inferencia.

En el numeral Noveno de los *Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, se*

enmarcan las reglas a seguir para los casos concretos en los que se solicite un documento o expediente que contenga partes o secciones clasificadas, los titulares de las áreas deberán elaborar una versión pública fundando y motivando la clasificación de las partes o secciones **que deban testarse**, siguiendo los procedimientos establecidos en el Capítulo IX.

Que a saber, dispone lo siguiente:

*“Quincuagésimo noveno. En caso de que el documento únicamente se posea versión impresa, deberá fotocopiar y sobre éste **deberán testarse** las palabras, párrafos o renglones que sean clasificados, debiendo anotar al lado del texto omitido, una referencia numérica tal y como se puede observar en el modelo para testar documentos impresos contenido en el Anexo 1 de los Lineamientos, “Modelo para testar documentos impresos”...*

*Sexagésimo. En caso de que el documento se posea en formato electrónico, deberá crearse un nuevo archivo electrónico para que sobre el mismo se elabore la versión pública, **eliminando las partes o secciones clasificadas**, de acuerdo con el modelo para testar documentos electrónicos contenido en el Anexo 2 de los Lineamientos, “Modelos para testar documentos electrónicos”.*”

Derivado de lo anterior, cabe decir que en términos de la fracción XVII del numeral segundo de los Lineamientos de referencia, la acción **testar**, corresponde a *la omisión o supresión de la información clasificada como reservada o confidencial, empleando sistemas o medios que impidan la recuperación o visualización de ésta.*

Por lo que se concluye, que cuando se ordena testar la información se atiende a un proceso de clasificación de la información y no al tratamiento de datos personales mediante la técnica de disociación.

Sin soslayar, que en el tratamiento de los datos personales de los miembros de cuerpos de seguridad pública, deberá emplearse el procedimiento para la anonimización mediante sus técnicas para salvaguardar la integridad física del elemento de seguridad pública y su familia.

En el tratamiento de datos personales deberá garantizarse el ejercicio del derecho de acceso a la información, y salvaguardar la integridad de los cuerpos de seguridad pública, al implementarse en todo caso, algoritmos y claves en los nombres de éstos, sin que se determine la clasificación de la información.

Por las consideraciones expuestas anteriormente formulo el presente **VOTO PARTICULAR**, en los términos precisados.

**Javier Martínez Cruz**  
Comisionado  
(Rúbrica)

