

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 NOVENA SESIÓN ORDINARIA DEL ONCE DE MARZO DE DOS MIL VEINTE, EN EL RECURSO DE REVISIÓN 09788/INFOEM/IP/RR/2019 Y ACUMULADOS.

Con fundamento en lo dispuesto por el artículo 14, fracciones X y XI, del Reglamento del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México, el Comisionado Javier Martínez Cruz emite **VOTO PARTICULAR** respecto a la resolución dictada en el recurso de revisión número 09788/INFOEM/IP/RR/2019 y Acumulados, pronunciada por el Pleno de este Instituto ante el proyecto presentado por el Comisionado José Guadalupe Luna Hernández, que es del tenor siguiente:

De las solicitudes de información se destaca que el particular requirió sustancialmente información relacionada con el organigrama del municipio; los recibos de nómina del personal de diversas áreas administrativas, así como el título universitario y cédula de los Directores, entre ellos el de Seguridad Pública.

El Sujeto Obligado respondió respecto al organigrama, que éste se encuentra publicado en una dirección electrónica la cual proporcionó y adjuntó el documento que lo contiene.

En cuanto a los recibos de nómina, proporcionó diversos listados que contienen el cargo, departamento, el total bruto y total neto de las áreas y periodos solicitados.

Por lo que hace a los títulos y cédulas profesionales solicitados, sólo envió el correspondiente del Director de Desarrollo Económico.

Inconforme, con las respuestas la Recurrente interpuso los recursos de revisión materia de análisis, en el que se inconformó sustancialmente por las respuestas incompletas.

Por su parte, el Sujeto Obligado omitió rendir sus respectivos informes justificados.

Finalmente, la Ponencia resolvió **modificar** las respuestas del Sujeto Obligado y en su resolutivo **SEGUNDO** ordenó la entrega, previa búsqueda exhaustiva y razonable, de ser procedente en versión pública, de la "Estructura Orgánica del Municipio de Axapusco, actualizada al veintiséis (26) de noviembre de dos mil diecinueve"; "Título y cédula profesional del Director de Desarrollo Social, del Director de Desarrollo Económico y del Director de Servicios Públicos del Municipio de Axapusco" y los "Recibos de nómina" del personal adscrito a diversas áreas administrativas, del Sujeto

Obligado, entre ellas, de la Dirección de Seguridad Pública del Municipio de Axapusco.

Determinación con la que el suscrito está de acuerdo, no obstante, por cuanto a la información relacionada con la Dirección de Seguridad Pública, la Resolutora determinó que ésta deberá entregarla de forma disociada en los términos siguientes:

*“En ese sentido la documentación que deberá proporcionar el **SUJETO OBLIGADO**, con los datos disociados podrá consistir en una lista de servidores públicos por orden alfabético sin especificar cargos y el tabulador de sueldos en donde sea visible el cargo y la remuneración de los servidores públicos adscritos a la Dirección de Seguridad Pública.”*

En esta tesitura, el contenido del voto particular emitido por el suscrito radica en la interpretación que la Ponencia encargada del análisis y resolución del presente asunto otorga al término “disociación de datos personales”, toda vez que en su estudio la determinó como una mera separación de dos documentos, es decir, un listado y el tabulador de sueldos.

No se puede perder de vista que estamos en una materia de contenido técnico, por lo tanto, debe atenderse a la definición del término “disociación”, establecida por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados:

XIII. Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

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.”

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, incluye 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 sometán 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

...”

De lo citado con antelación, se deduce que una disociación responde a un tratamiento de datos personales efectuado mediante procedimientos manuales o automatizados que buscan la separación de la información pero aún es posible una inferencia, ahora bien, en el caso concreto, lo que pretendieron proteger por medio de este proceso, son los nombres o la identificación de los policías.

Sin embargo, a consideración del suscrito, los nombres de los servidores públicos son de carácter público por regla general, así lo sustenta el artículo 92, fracciones II, VII y VIII de la legislación aplicable a la materia, mismo que se cita a continuación:

“Artículo 92. Los sujetos obligados deberán poner a disposición del público de manera permanente y actualizada de forma sencilla, precisa y entendible, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas que a continuación se señalan:

II. Su estructura orgánica completa, en un formato que permita vincular cada parte de la estructura, las atribuciones y responsabilidades que le corresponden a cada servidor público, prestador de servicios profesionales o miembro de los sujetos obligados, de conformidad con las disposiciones jurídicas aplicables;

VII. El directorio de todos los servidores públicos, a partir del nivel de jefe de departamento o su equivalente o de menor nivel, cuando se brinde atención al público, manejen o apliquen recursos públicos, realicen actos de autoridad o presten servicios profesionales bajo el régimen de confianza u honorarios y personal de base.

El directorio deberá incluir, al menos el nombre, cargo o nombramiento oficial asignado, nivel del puesto en la estructura orgánica, fecha de alta en el cargo, número telefónico, domicilio para recibir correspondencia y dirección de correo electrónico oficiales, datos que deberán señalarse de forma independiente por dependencia y entidad pública de cada sujeto obligado;

VIII. La remuneración bruta y neta de todos los servidores públicos de base o de confianza, de todas las percepciones, incluyendo sueldos, prestaciones, gratificaciones, primas, comisiones, dietas, bonos, estímulos, ingresos y sistemas de compensación, señalando la periodicidad de dicha remuneración;

...”

No pasa inadvertido para el emisor de este voto particular que existen criterios de excepción en la legislación aplicable en la materia, el numeral 140 de la multicitada legislación local enlista las causales en las que de configurarse el hecho con la hipótesis normativa podrá clasificarse el nombre de los policías:

“Artículo 140. El acceso a la información pública será restringido excepcionalmente, cuando por razones de interés público, ésta sea clasificada como reservada, conforme a los criterios siguientes:

[...]

IV. Ponga en riesgo la vida, la seguridad o la salud de una persona física;

...”

(Énfasis añadido)

Bajo este orden de ideas, la Corte Interamericana de Derechos Humanos, establece que corresponde al Estado la carga probatoria para limitar el derecho de acceso a la información del ciudadano, además las Relatorías para la Libre Expresión advierten que ante un conflicto de normas, deberá atenderse a lo dispuesto por la legislación en materia de acceso a la información pública:

“La jurisprudencia de la Corte Interamericana ha establecido que el Estado tiene la carga de la prueba de demostrar que las limitaciones al acceso a la información son compatibles con las normas interamericanas sobre libertad de expresión. Así también lo ha afirmado el Comité Jurídico Interamericano en su resolución sobre los “Principios sobre el Derecho de Acceso a la Información.”

Tal como ha sido ampliamente reconocido en el seno de las relatorías para la libertad de expresión, frente a un conflicto de normas, la ley de acceso a la información deberá prevalecer sobre toda otra legislación. Lo anterior, toda vez que se ha reconocido al derecho de acceso a la información como un requisito indispensable para el funcionamiento mismo de la democracia. Esta exigencia ayuda a promover que los Estados cumplan efectivamente con la obligación de establecer una ley de acceso a la información pública y a que la interpretación de la misma resulte efectivamente favorable al derecho de acceso”¹.

Igualmente, señala en su documento que los relatores para la libertad de expresión de la ONU, OEA Y OSCE han formulado una síntesis de los requisitos que deben cumplir las limitaciones al derecho de acceso a la información, y profundizaron en

¹ El derecho de acceso a la información en el marco jurídico interamericano. CIDH (2010).OEA,pp.4

algunos temas atinentes a la información “reservada” o “secreta” y las leyes que establecen tal carácter, así como los funcionarios obligados legalmente a guardar su carácter confidencial. Por lo tanto en términos generales establecen lo siguiente:

- (I) que “el derecho de acceso a la información deberá estar sujeto a un sistema restringido de excepciones cuidadosamente adaptado para proteger los intereses públicos y privados preponderantes, incluida la privacidad”, que “las excepciones se aplicarán solamente cuando exista el riesgo de daño sustancial a los intereses protegidos y cuando ese daño sea mayor que el interés público en general de tener acceso a la información”, y que “la autoridad pública que procure denegar el acceso debe demostrar que la información está amparada por el sistema de excepciones”;
- (II) que “aquéllos que soliciten información deberán tener la posibilidad de apelar cualquier denegación de divulgación de información ante un órgano independiente con plenos poderes para investigar y solucionar dichos reclamos”; y que
- (III) “las autoridades nacionales deberán tomar medidas activas a fin de abordar la cultura del secretismo que todavía prevalece en muchos países dentro del sector público”, lo cual “deberá incluir el establecimiento de sanciones para aquellos que deliberadamente obstruyen el acceso a la información”, y que “también se deberán adoptar medidas para promover una amplia sensibilización pública sobre la ley de acceso a la información”

Aunado a lo anterior, la legislación local vigente dispone que la clasificación de la información no se da exclusivamente por la existencia del mandato de la ley, para ello, el Estado atribuye al Sujeto Obligado la carga probatoria a efecto de determinar mediante la aplicación de la prueba de daño correspondiente si su divulgación representa un riesgo real y demostrable para la seguridad pública:

“Artículo 129. En la aplicación de la prueba de daño, el sujeto obligado deberá precisar las razones objetivas por las que la apertura de la información generaría una afectación, justificando que:

I. La divulgación de la información representa un riesgo real, demostrable e identificable del perjuicio significativo al interés público o a la seguridad pública;

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda; y

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio

Artículo 131. La carga de la prueba para justificar toda negativa de acceso a la información, por actualizarse cualquiera de los supuestos de clasificación previstos en esta Ley corresponderá a los sujetos obligados; en tal caso deberá fundar y motivar debidamente la clasificación de la información, de conformidad con lo previsto en la presente Ley.”

En este tenor, los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, contemplan los casos específicos en los cuales deberá configurarse

estrictamente el posible menoscabo para estimarse procedente la reserva de la información:

“Décimo octavo. De conformidad con el artículo 113, fracción I² de la Ley General, podrá considerarse como información reservada, aquella que comprometa la seguridad pública, al poner en peligro las funciones a cargo de la Federación, la Ciudad de México, los Estados y los Municipios, tendientes a preservar y resguardar la vida, la salud, la integridad y el ejercicio de los derechos de las personas, así como para el mantenimiento del orden público.

Se pone en peligro el orden público cuando la difusión de la información pueda entorpecer los sistemas de coordinación interinstitucional en materia de seguridad pública, menoscabar o dificultar las estrategias contra la evasión de reos; o menoscabar o limitar la capacidad de las autoridades encaminadas a disuadir o prevenir disturbios sociales.

Asimismo, podrá considerarse como reservada aquella que revele datos que pudieran ser aprovechados para conocer la capacidad de reacción de las instituciones encargadas de la seguridad pública, sus planes, estrategias, tecnología, información, sistemas de comunicaciones.”

(Énfasis añadido)

Precisado lo anterior, se concluye que es posible restringir el ejercicio de un derecho siempre y cuando obre la fundamentación y motivación adecuada, lo anterior se sustenta en la siguiente tesis:

² Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:
I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;

“FUNDAMENTACIÓN Y MOTIVACIÓN DE LOS ACTOS ADMINISTRATIVOS. De acuerdo con el artículo 16 constitucional, todo acto de autoridad debe estar suficientemente fundado y motivado, entendiéndose por lo primero que han de expresarse con precisión el precepto legal aplicable al caso y por lo segundo, que también deben señalarse con precisión, las circunstancias especiales, razones particulares o causas inmediatas que se hayan tenido en consideración para la emisión del acto, siendo necesario además, que exista adecuación entre los motivos aducidos y las normas aplicables, es decir, que en el caso concreto se configure la hipótesis normativa. Esto es, que cuando el precepto en comento previene que nadie puede ser molestado en su persona, propiedades o derechos sino en virtud de mandamiento escrito de autoridad competente que funde y motive la causa legal del procedimiento, está exigiendo a todas las autoridades que apeguen sus actos a la ley, expresando de que ley se trata y los preceptos de ella que sirvan de apoyo al mandamiento relativo. En materia administrativa, específicamente, para poder considerar un acto autoritario como correctamente fundado, es necesario que en él se citen: a).- Los cuerpos legales y preceptos que se estén aplicando al caso concreto, es decir, los supuestos normativos en que se encuadra la conducta del gobernado para que esté obligado al pago, que serán señalados con toda exactitud, precisándose los incisos, subincisos, fracciones y preceptos aplicable, y b).- Los cuerpos legales y preceptos que otorgan competencia o facultades a las autoridades para emitir el acto en agravio del gobernado.”

Lo anterior, son razones suficientes para la emisión y presentación del presente Voto Particular relacionado con la resolución del recurso de revisión referido.

Javier Martínez Cruz
Comisionado
(Rúbrica)