EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN MATERIA PENAL

Roberto Orozco Martínez*

* Director de Verificación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

PALABRAS CLAVE *KEYWORDS*

Datos personales	*Personal data*
Derechos ARCO	*ARCO Rights*
Tratamiento	*Treatment*
Responsable	*Responsible*

Resumen. El derecho a la protección de datos personales constituye un derecho fundamental, reconocido constitucionalmente, que supone la posibilidad de elegir qué información de la esfera privada de la persona puede ser conocida, así como decidir quién puede usar dicha información y bajo qué condiciones, así como la facultad de acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales en posesión de personas físicas y/o morales de carácter privado, así como de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito federal, estatal y municipal, lo cual comprende las instancias administrativas y jurisdiccionales en materia penal, es decir, aquellas encargadas de la investigación y persecución de delitos y la imposición de penas.

Abstract. The right to the protection of personal data constitutes a fundamental right, constitutionally recognized, that supposes the possibility of choosing which information of the private sphere of the person can be known, as well as deciding who can use such information and under what conditions; it also gives the right to access, rectify, cancel and oppose the processing of their personal data held by private individuals and / or corporations, as well as any authority, entity, body and agency of the Executive, Legislative and Judicial Powers, autonomous organs, political parties, trusts and public funds, in the federal, state and municipal levels, which includes the administrative and jurisdictional instances in criminal matters, that is, those in charge of the investigation and prosecution of crimes and the imposition of penalties.

SUMARIO:

I. INTRODUCCIÓN

Con el desarrollo y evolución de las tecnologías de la información y el comercio internacional globalizado, el flujo de información se ha visto incrementado exponencialmente, incluyendo datos personales, puesto que los medios tradicionales de comunicación han sido desbordados por las modalidades y mecanismos proporcionados por los adelantos científicos y tecnológicos.

La utilización de nuevas tecnologías facilita la obtención, utilización y almacenamiento de grandes cantidades de información y datos personales, de forma sistematizada y automatizada en espacios reducidos y con disponibilidad inmediata; lo anterior representa un riesgo latente frente al derecho a la protección de datos personales, ante lo cual las instituciones gubernamentales deben actuar para garantizar el cumplimiento de los derechos fundamentales de las personas.

En esa tesitura, el primer ordenamiento legal promulgado en la República Mexicana que contempló la materia de protección de datos personales fue la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el *Diario Oficial de la Federación* el 11 de julio de 2002, la cual tuvo como finalidad regular el derecho de acceso a la información, previendo la protección de datos personales como una limitación al referido derecho, al considerarlos como información confidencial. Asimismo, la Ley Federal mencionada incluyó un capítulo de protección de datos personales, en el que se establecieron las primeras nociones de los principios básicos que se consideró debían regir el tratamiento de los mismos, así como prevenciones generales que dieron origen a los derechos de acceso y rectificación de datos personales.

No obstante, hasta la reforma del artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, publicada el 20 de julio de 2007 en el *Diario Oficial de la Federación*, a través de la cual se adicionó un segundo párrafo con siete fracciones, se reconoció como derecho fundamental la protección de datos personales, así como los diversos de acceso y rectificación, en los siguientes términos:

> Artículo 6.-…
> Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
> …
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos…

De esa forma, puede considerarse que se dio el primer paso al reconocer con una mención expresa el derecho

a la protección de datos personales como un derecho fundamental en la Constitución Política de los Estados Unidos Mexicanos para que, a partir de ello, pudiera continuar el desarrollo de la normatividad que regula la materia.

Ahora bien, mediante el Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, se adicionó la fracción VIII al artículo 6o, estableciendo que la Federación contaría con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.

De igual forma, se adicionó, entre otras, la fracción XXIX-S al artículo 73, otorgando al Congreso de la Unión la facultad para expedir las leyes generales reglamentarias para el desarrollo de los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno.

Derivado de lo anterior, el 26 de enero de 2017 se publicó en el *Diario Oficial de la Federación*, el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual entró en vigor al día siguiente de su publicación, y que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados, entre los cuales se encuentran las instancias administrativas y jurisdiccionales encargadas de la persecución e investigación de conductas probablemente constitutivas de delitos, así como las encargadas de imponer penas.

II. MARCO LEGAL DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

El marco jurídico que actualmente regula el derecho fundamental a la protección de los datos personales en México, se encuentra constituido, en principio, por los artículos 6, apartado A, y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como las disposiciones reglamentarias, lineamientos y demás normativa que de ellas derivan.

Sin embargo, considerando que el presente documento se enfoca a la protección de datos personales en materia penal, se estima pertinente obviar el contenido de la normativa aplicable a particulares, toda vez que el tratamiento que llevan a cabo las autoridades administrativas y jurisdiccionales para la investigación y persecución de delitos, así como la imposición de penas en un

proceso criminal a la luz del derecho a la protección de los datos personales, es el tema relevante.

No debe perderse de vista que en términos de los artículos Primero y Cuarto Transitorios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dicho ordenamiento se encuentra vigente desde el 27 de enero de 2017, quedando derogadas todas aquellas disposiciones en materia de protección de datos personales, de carácter federal, estatal y municipal, que contravengan lo dispuesto por la referida Ley.

Aunado a lo anterior, es importante destacar que el 26 de enero de 2018, se publicaron en el *Diario Oficial de la Federación* los Lineamientos Generales de Protección de Datos Personales para el Sector Público, los cuales tienen por objeto desarrollar las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en lo relativo al ámbito federal.

Precisado lo anterior, resulta conveniente proceder a la explicación de los ámbitos subjetivo, objetivo y territorial de validez de la normatividad aplicable en materia de protección de datos personales a las instancias administrativas y jurisdiccionales en materia penal.

Para tal efecto, los artículos 1, párrafos primero, segundo y quinto, y 4 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, disponen que se trata de un ordenamiento de observancia general en toda la República Mexicana (ámbito territorial), de aplicación directa para los sujetos obligados pertenecientes al orden federal, es decir, a cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos (ámbito subjetivo), respecto de cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización (ámbito objetivo).

Los artículos 3 y 4 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establecen que serán aplicables a cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos del ámbito federal (ámbito subjetivo), en relación con el tratamiento de datos personales de personas físicas que obren en soportes físicos y/o electrónicos, ya que los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o en cualquier otro formato (ámbito objetivo).

Lo anterior implica que las autoridades administrativas, como la Procuraduría General de la República, los Ministerios Públicos Federales y sus fiscalías especializadas, la Policía Federal; y las integrantes del Poder Judicial de la Federación, como pueden ser de manera enunciativa, los Juzgados de Distrito, los Tribunales Unitarios y Colegiados de Circuito, así como todos y cada uno de los funcionarios de mando y operativos, adscritos a dichas instancias gubernamentales, se encuentran obligados a garantizar el derecho a la protección de los datos personales

que utilizan diariamente para el desempeño de sus actividades, en todo el territorio de los Estados Unidos Mexicanos en el ámbito Federal, respecto del tratamiento que lleven a cabo, independientemente del medio físico y/o electrónico en que se encuentren contenido los datos personales.

Esto es, el derecho a la protección de los datos personales y el ejercicio de los derechos ARCO que será explicado en párrafos posteriores, abarca no solo los documentos físicos y constancias contenidas en los diversos expedientes, carpetas de investigación, juicios penales y medios de impugnación interpuestos, sino también se extiende a las bases de datos, equipos de cómputo con que cuentan los sujetos obligados, incluyendo también, las grabaciones, videos, fotografías y toda clase de elementos probatorios aportados y facilitados por los descubrimientos de la ciencia y avances tecnológicos, siempre y cuando se refieran a personas físicas identificadas o identificables, ya sean víctimas, testigos, peritos, imputados, etcétera.

III. LOS PRINCIPIOS Y DEBERES EN EL TRATAMIENTO DE DATOS PERSONALES EN MATERIA PENAL

Ahora bien, antes de proceder a explicar los principios, deberes y derechos que comprende el derecho a la protección de datos personales, debe aclararse un concepto fundamental denominado "tratamiento" que, en términos de lo dispuesto por el artículo 3, fracción XXXIII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, consiste en cualquier operación o conjunto de operaciones efectuadas mediante 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.

De tal manera, ante la generalidad y amplia gama de acciones que abarca el tratamiento de los datos personales, puede notarse claramente que cualquier tipo de actividad que se efectúe con datos personales, conlleva la aplicación y estricto cumplimiento a la normatividad en la materia.

En efecto, la presentación de una denuncia de hechos ante un Agente del Ministerio Público implica la obtención y registro de datos personales, al menos de carácter identificativo (nombre, domicilio, edad, sexo, entre otros); la conservación y archivo de una carpeta de investigación o el expediente de una causa penal, significa el almacenamiento de datos personales; la consignación ante un juez de control, para que determine la situación jurídica de un imputado, o la remisión de un expediente a un Tribunal Colegiado o Unitario para que resuelva un medio de impugnación, puede configurar una transferencia de datos personales; sin mencionar la diversidad de información y datos personales que pueden presentarse, obtenerse y aportarse durante la sustanciación

de un proceso penal a través de pruebas periciales o inspecciones.

Por tal motivo, los responsables del tratamiento de toda esta categoría de información, identificada como "datos personales", deben tomar en cuenta las modificaciones referidas al orden jurídico nacional y local en la materia, para asegurarse de establecer e implementar las medidas y acciones necesarias a efecto de estar en posibilidad jurídica y materialmente de garantizar el pleno ejercicio de los derechos y cumplir con las obligaciones instituidas a partir de la entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Conviene señalar que de conformidad con los artículos 16 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; y 7 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público; en todo tratamiento de datos personales, los responsables deben observar los principios rectores de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; razón por la cual a continuación se procede a efectuar una breve explicación de las implicaciones generales que tiene el cumplimiento de cada uno de ellos por parte de algunas de las autoridades competentes en materia penal, sin perder de vista que las obligaciones resultantes se encuentran estrechamente vinculadas, por lo que no deben verse de forma aislada, pues generalmente el incumplimiento de alguno impacta indefectiblemente en otros.

El principio de licitud, previsto en los artículos 17 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 8 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, dispone que el responsable debe tratar los datos personales sujetándose a las facultades o atribuciones que la normatividad aplicable le confiera, así como con estricto apego y en cumplimiento a lo dispuesto por la legislación mexicana y, en su caso, el derecho internacional.

La situación anterior se relaciona estrechamente con el régimen de facultades expresas que rige la actuación de las autoridades, toda vez que solo pueden realizar aquello para lo que están expresamente autorizadas por las leyes, como consecuencia indisoluble del derecho a la seguridad jurídica y el principio de legalidad que reconoce el texto constitucional; lo cual ha sido ampliamente estudiado por diversos criterios sustentados por el Poder Judicial de la Federación e inclusive por la propia Suprema Corte de Justicia de la Nación.

En tal virtud, lo primero que debe tomarse en cuenta es que la normatividad que regula la actuación de cada una de las instancias administrativas y jurisdiccionales, tales como Leyes Orgánicas, Códigos Penales y de Procedimientos Penales, Lineamientos, Acuerdos Delegatorios, Reglamentos Interiores, por mencionar algunos, prevean facultades expresas para llevar a cabo el tratamiento de los datos personales que pretenden realizar, para que

estén en aptitud de efectuarlo de forma lícita.

Del mismo modo, en cumplimiento del principio de finalidad, todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas (cuando se atiende a la consecución de fines específicos), lícitas (cuando los fines son acordes a las atribuciones y facultades del responsable), explícitas (cuando se expresan y se dan a conocer de forma clara en el aviso de privacidad) y legítimas (cuando las finalidades se encuentran habilitadas por el consentimiento del titular o alguna causal de excepción), relacionadas con las atribuciones que la normatividad aplicable les confiera.

En ese orden de ideas, las finalidades del tratamiento de los datos personales deben estar relacionadas y ser congruentes con las facultades y atribuciones legales de cada sujeto obligado responsable, conforme al marco legal que delimita su ámbito de competencia, lo cual se relaciona con el cumplimiento del principio de licitud.

Asimismo, las características que deben cubrir las finalidades del tratamiento para que sean explícitas y legítimas, se vinculan con el cumplimiento de los diversos principios de información y consentimiento, por lo que se reitera, las obligaciones derivadas de los principios rectores del derecho a la protección de datos personales deben estudiarse de forma conjunta y no de manera independiente, pues tienen múltiples puntos de contacto entre sí.

El principio de consentimiento, referido en el párrafo que antecede, se encuentra previsto en los artículos 20 y 21 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 12 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, y establece que, previo al tratamiento, los responsables deben obtener el consentimiento del titular para el tratamiento de sus datos personales, entendido como la manifestación de voluntad de manera libre (sin que medie error, mala fe, violencia o dolo), específica (referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento) e informada (cuando se tenga conocimiento del aviso de privacidad previo al tratamiento).

Cabe destacar que una de las particularidades que se presentan del derecho a la protección de datos personales en posesión de los sujetos obligados del sector público, incluyendo instancias administrativas y jurisdiccionales competentes en materia penal, en contraposición al sector privado, es que en este último caso, es regla general la necesidad de obtener el consentimiento de los titulares para autorizar y legitimar el tratamiento de sus datos personales; mientras que tratándose de instancias gubernamentales, por revestir el carácter de autoridades regidas por un marco normativo que regula su esfera de competencia, muchos de los casos podrían actualizar alguna de las hipótesis de excepción al principio de información.

En otras palabras, el artículo 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece supuestos en los cuales los responsables no están obligados a recabar el consentimiento del titular para el tratamiento de sus datos personales, por ejemplo: cuando una

ley así lo disponga, cuando las transferencias que se realicen entre responsables, y sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien, cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.

Por otra parte, en relación con el principio de información, establecido en los artículos 26 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 26 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, los responsables deben informar a los titulares, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos los datos personales, con el objeto que puedan tomar decisiones informadas al respecto, lo cual también incide en el cumplimiento de los diversos principios de finalidad, consentimiento e, incluso, el de lealtad.

En ese tenor, el aviso de privacidad es definido como el documento que es puesto disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Resulta relevante destacar que de acuerdo con el artículo 26, párrafo segundo, de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, todo responsable está obligado a cumplir con el principio de información, poniendo a disposición del titular el aviso de privacidad respectivo, con independencia de que no se requiera su consentimiento para el tratamiento de sus datos personales.

Por lo tanto, si bien una autoridad administrativa y/o jurisdiccional podría estar facultada para realizar el tratamiento de datos personales con motivo de una disposición legal que les otorga atribuciones en ese sentido, por ejemplo, para instaurar una carpeta de investigación, radicar, sustanciar y resolver un proceso penal, lo cierto es que ello no exime de la obligación de poner a disposición de los titulares el aviso de privacidad correspondiente.

Ahora bien, el principio de lealtad conlleva que el responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos (aquellos que el responsable utilice para tratar datos personales con dolo, mala fe o negligencia), privilegiando la protección de los intereses del titular (cuando el tratamiento de los datos personales que efectúa el responsable no da lugar a discriminación, un trato injusto o arbitrario contra el titular) y la expectativa razonable de privacidad (entendida como la confianza que el titular deposita en el responsable respecto de que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones legales correspondientes); lo anterior, acorde a lo previsto en los artículos 19 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 11 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

En cambio, en cumplimiento al principio de calidad, los artículos 23 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 21 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, disponen que los responsables deberán adoptar las medidas necesarias para mantener exactos y correctos (cuando los datos no presentan errores), completos (cuando la integridad de los datos personales permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable) y actualizados (cuando responden fielmente a la situación actual del titular) los datos personales en su posesión, a fin de que no se altere la veracidad de estos.

Lo anterior reviste especial relevancia en materia penal, toda vez que las autoridades administrativas como la Procuraduría General de la República, Ministerios Públicos y Policía Federal tienen que asegurarse de que los datos personales que obtienen y utilizan cumplan con las características referidas en el párrafo que precede, ya que la inexactitud o falta de actualización de los mismos, puede traer consecuencias que afecten la libertad y condición jurídica de víctimas e imputados; asimismo, si los datos personales contenidos en los expedientes de procesos penales son incorrectos o incompletos, pueden ocasionar la emisión de actuaciones y sentencias que deparen perjuicios en la esfera jurídica de los imputados o causar inconsistencias en las bases de datos y registros que utiliza el sistema penitenciario.

Por otro lado, también se debe considerar el principio de proporcionalidad, el cual de acuerdo con los artículos 25 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 24 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, conlleva tratar solo los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento, es decir, cuando son apropiados, indispensables y no excesivos en términos de las atribuciones conferidas al responsable.

La redacción anterior de la ley de la materia y la normatividad que de ella deriva, no es clara en definir lo que debe entenderse por adecuados, apropiados, relevantes, indispensables, estrictamente necesarios y no excesivos, por lo que desafortunadamente pareciera existir un margen de interpretación que puede dar lugar a la aplicación subjetiva de las obligaciones que genera el cumplimiento del principio de proporcionalidad; sin embargo, con el afán de establecer un parámetro objetivo a partir del cual pudiera determinarse si un dato personal resulta proporcional o no, y así brindar certeza jurídica a los responsables, los primeros dos aspectos que tendrían que considerarse son las disposiciones legales y requisitos establecidos en la normatividad sustantiva y adjetiva en materia penal para el tratamiento que haya de llevarse a cabo, y, en segundo término, lo estipulado en los avisos de privacidad correspondientes.

Es necesario analizar casuísticamente los asuntos que pudieran presentarse, para poder definir, en atención a todas y cada una de las particularidades que envuelven el tratamiento de los datos personales que se desarrolle y la

situación en que se encuentra el titular, si los responsables dan cumplimiento o no al principio de proporcionalidad, así como a los demás principios referidos previamente.

Finalmente, el principio de responsabilidad previsto en los artículos 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 56 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, conlleva la obligación de implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y obligaciones establecidos y rendir cuentas sobre el tratamiento de datos personales en su posesión.

Para tal efecto, la normatividad en materia de protección de datos personales en el sector público, refiere diversas acciones mínimas que deben adoptar los responsables para cumplir con el principio de responsabilidad, a saber: destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales; poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales; establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales; diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la ley de la materia y las demás que resulten aplicables, entre otras.

Aunado a lo expuesto con anterioridad, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público establecen la obligación de los responsables de dar cumplimiento a los deberes de confidencial y de seguridad.

El deber de seguridad establecido en los artículos 31 a 41 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 55 a 70 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, implica que, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable debe establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

De ese modo, las instancias administrativas y jurisdiccionales competentes en materia penal, deben llevar a cabo las adecuaciones normativas y organizacionales que estimen necesarias para el establecimiento y efectiva implementación de las medidas de seguridad respectivas, lo cual debe estar contenido en un "documento de seguridad" que contenga el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; el

análisis de riesgos que incluya las consecuencias negativas para los titulares que pudieran derivar de una vulneración; el análisis de brecha, abarcando las medidas de seguridad existentes y faltantes; el plan de trabajo que defina las acciones a realizar de acuerdo al resultado del análisis de riesgos y de brecha; los mecanismos de monitoreo y revisión de las medidas de seguridad; y el programa general de capacitación.

Las medidas de seguridad de carácter físico son las acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, lo cual puede ser tan simple como la instalación de puertas para el control de acceso a las instalaciones y oficinas en un Ministerio Público o un juzgado, la utilización de credenciales para identificar al personal autorizado, hasta el mantenimiento de mobiliario, archiveros y equipos informáticos que contienen o almacenan datos personales.

Las medidas de seguridad de carácter administrativo son las diversas políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales, como pueden ser los manuales de procedimientos y de organización que delimiten las actividades que involucran el tratamiento de datos personales y las responsabilidades de cada uno de los servidores públicos que participan, incluyendo políticas de conservación de archivos físicos y electrónicos, así como cursos y talleres de formación en la materia.

Las medidas de seguridad técnicas, las cuales resultan especialmente relevantes en la actualidad debido al alto nivel de automatización y sistematización de los procedimientos y bases de datos con que cuentan las instancias administrativas y jurisdiccionales competentes en materia penal, involucran las acciones y mecanismos que utilizan la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De tal suerte, los responsables deben prever, por ejemplo, el establecimiento de usuarios y contraseñas para el acceso a equipos de cómputo, un esquema de autorizaciones y privilegios para el desarrollo de actividades que requiere cada funcionario, y el establecimiento de configuraciones tales como mecanismos de cifrado, para garantizar las comunicaciones y operaciones de los recursos informáticos en el tratamiento de datos personales.

Por otra parte, en cumplimiento al deber de confidencialidad establecido en los artículos 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y 71 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, los responsables deben establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de estos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

En relación con lo anterior, el artículo 106 del Código Nacional

de Procedimientos Penales, en vigor a nivel federal a partir del 29 de abril de 2016 de conformidad con la Declaratoria por la que el Congreso de la Unión declara la entrada en vigor a nivel federal del Código Nacional de Procedimientos Penales, a partir del 29 de abril de 2016, en los estados de Campeche, Michoacán, Sonora y Veracruz; y a partir del 14 de junio de 2016 en los estados de Baja California, Guerrero, Jalisco, Tamaulipas, así como en el archipiélago de las Islas Marías y en el resto del territorio nacional, a que se refieren los artículos 42 y 48 de la Constitución Política de los Estados Unidos Mexicanos, publicada en el *Diario Oficial de la Federación* el 26 de febrero de 2016, en relación con el Artículo Segundo Transitorio del Decreto por el que se expide el Código Nacional de Procedimientos Penales, publicado en el *Diario Oficial de la Federación* el 5 de marzo de 2014; dispone lo siguiente:

> Artículo 106. Reserva sobre la identidad
> En ningún caso se podrá hacer referencia o comunicar a terceros no legitimados la información confidencial relativa a los datos personales de los sujetos del procedimiento penal o de cualquier persona relacionada o mencionada en éste.
> Toda violación al deber de reserva por parte de los servidores públicos, será sancionada por la legislación aplicable.
> En los casos de personas sustraídas de la acción de la justicia, se admitirá la publicación de los datos que permitan la identificación del imputado para ejecutar la orden judicial de aprehensión o de comparecencia.

Por tal motivo, es claro que la propia normativa específica en materia penal contempla la prohibición de hacer referencia o comunicar a terceros no legitimados la información relativa a los datos personales de los sujetos del procedimiento penal o de cualquier persona relacionada o mencionada en este.

Ello, sin perjuicio de la obligación de establecer las medidas o controles que los responsables estimen pertinentes a efecto de garantizar que quienes participan en cualquier etapa del tratamiento de datos personales, guarden confidencialidad, no solo respecto de la identidad de los sujetos en un proceso penal, sino de toda la información concerniente a toda persona física identificada o identificable, aun con posterioridad a que concluyan el desempeño de su cargo como servidores públicos.

IV. FUENTES DE CONSULTA

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el *Diario Oficial de la Federación* el 11 de junio de 2002. Disponible en www.diputados.gob.mx/LeyesBiblio/abro/lftaipg.htm, y actualmente abrogada por virtud del Decreto por el que se abroga la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se expide la Ley Federal de Transparencia y Acceso a la Información Pública, publicado en el *Diario Oficial de la Federación* el 9 de mayo de 2016. Disponible en www.diputados.gob.mx/ LeyesBiblio/abro/lftaipg/LFTAIPG_abro_09may16.pdf.

Decreto por el que se adiciona un segundo párrafo con siete fracciones

al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, publicado en el *Diario Oficial de la Federación* el 20 de julio de 2017. Disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_174_20jul07_ima.pdf.

Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, publicado en el *Diario Oficial de la Federación* el 7 de febrero de 2014. Disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf.

Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicado en el *Diario Oficial de la Federación* el veintiséis de enero de dos mil diecisiete. Disponible en http://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017.

Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el *Diario Oficial de la Federación* el 26 de enero de 2018. Disponible en http://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha= 26/01/2018.

Declaratoria por la que el Congreso de la Unión declara la entrada en vigor a nivel federal del Código Nacional de Procedimientos Penales, a partir del 29 de abril de 2016, en los Estados de Campeche, Michoacán, Sonora y Veracruz; y a partir del 14 de junio de 2016 en los Estados de Baja California, Guerrero, Jalisco, Tamaulipas, así como en el archipiélago de las Islas Marías y en el resto del territorio nacional, a que se refieren los artículos 42 y 48 de la Constitución Política de los Estados Unidos Mexicanos, publicada en el *Diario Oficial de la Federación* el 26 de febrero de 2016. Disponible en www.diputados.gob.mx/LeyesBiblio/ref/cnpp/CNPP_decla06_ 26feb16.pdf.

Decreto por el que se expide el Código Nacional de Procedimientos Penales, publicado en el *Diario Oficial de la Federación* el 5 de marzo de 2014. Disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/cnpp/CNPP_orig_05mar14.pdf.

Código Nacional de Procedimientos Penales, cuyas últimas reformas fueron publicadas en el *Diario Oficial de la Federación* el 17 de junio de 2016. Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf.