



Publicación Cuatrimestral de Sociedad, Cultura y Desarrollo Sustentable

Ra Ximhai

ISSN: 1665-0441

raximhai@uaim.edu.mx

Universidad Autónoma Indígena de México
México

Hernández-Delgado, Vicente

Referentes legales para un marco protector de datos personales

Ra Ximhai, vol. 2, núm. 3, septiembre-diciembre, 2006, pp. 567-580

Universidad Autónoma Indígena de México

El Fuerte, México

Disponible en: <http://www.redalyc.org/articulo.oa?id=46120302>

- Cómo citar el artículo
- Número completo
- Más información del artículo
- Página de la revista en redalyc.org

redalyc.org

Sistema de Información Científica

Red de Revistas Científicas de América Latina, el Caribe, España y Portugal

Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Ra Ximhai

Revista de Sociedad, Cultura y Desarrollo
Sustentable

Ra Ximhai
Universidad Autónoma Indígena de México
ISSN: 1665-0441
México

2006

REFERENTES LEGALES PARA UN MARCO PROTECTOR DE DATOS PERSONALES

Vicente Hernández Delgado

Ra Ximhai, septiembre-diciembre, año/Vol.2, Número 3
Universidad Autónoma Indígena de México
Mochicahui, El Fuerte, Sinaloa. pp. 567-580



REFERENTES LEGALES PARA UN MARCO PROTECTOR DE DATOS PERSONALES

LEGAL REFERENTS TO A PERSONAL DATA PROTECTION FRAME

Vicente **Hernández-Delgado**

Comisionado Estatal de la Comisión Estatal para el Acceso a la Información Pública del Estado de Sinaloa (CEAIPES). Correo Electrónico: vhernandez@ceaipes.org.mx.

RESUMEN

El presente ensayo tiene como objetivo fundamental establecer un marco referencial que permita analizar los antecedentes normativos de la protección de los datos personales en nuestro país, planteando como punto de partida los antecedentes en la Constitución General de la Republica y en la legislación secundaria tanto de carácter federal como local, regulando los bienes jurídicos del derecho a la intimidad y la privacidad. En un plano intermedio, se aborda la influencia de las tecnologías de la información y comunicaciones en el nuevo marco regulador a nivel federal con la aparición de un nuevo lenguaje y figuras jurídicas en la legislación civil, mercantil, procesal y de protección al consumidor. Finalmente, la aparición de la legislación federal y locales en materia de acceso a la información y transparencia gubernamentales, la ley de protección de datos personales del Estado de Colima, así como la reglamentación respectiva por parte de la LFTAIP, permiten afirmar que de manera incipiente se ha comenzado a fomentar un marco protector de los datos personales en nuestro país.

Palabras clave: Aspectos legales, protección de datos personales, Acceso a la información.

SUMMARY

The present essay has as main target to establish a referential frame as much that it allows to analyze the normative Background of the protection of the personal data in our country, starting with antecedents in the General Republic Constitution and in the secondary legislation of federal and local character, regulating the legally protected interests of the right to the intimacy and the privacy. In an intermediate plane, the influence of the technologies of the information and communications in the new legal regulating frame is approached at federal level with the appearance of a new language and figures in the civil, mercantile, procedural and protection legislation of consumer. Finally, appearance of the federal and the local legislation in the matter of access to the governmental information and transparency, the law of protection of personal data of the state of Colima, as well as the respective regulation on the part of the LFTAIP, allows to affirm that on a weak way it has been begun to support a protective frame of the personal data in our country.

Key Words: Legal aspects, personal data protection, Information access.

INTRODUCCIÓN

A partir del auge de las tecnologías de la información, de manera particular la informática, telecomunicaciones y la ingeniería genética, sus efectos dinámicos en el procesamiento de la información y comunicación dan cuenta de la circulación de una gran variedad de datos mediante imágenes, textos, huella digital, DNA, mensajes, ideas, propuestas, informes, en donde el manejo de la información concerniente a la intimidad y la privacidad de las personas de parte de los usuarios y los responsables de los archivos o registros públicos y privados requiere de medidas de prevención y regulación mediante códigos de conductas éticas y legales procurando que tengan como prioridad la protección de los datos personales con la finalidad de asegurar el bien jurídico protegido por la ley: la intimidad y privacidad de las personas.

Rápidamente, de manera exponencial, la revolución de las tecnologías de la información contribuyó a modificar la cultura, las relaciones mercantiles y sociales de nuestro tiempo, generando nuevos tipos de conductas en función del uso o abuso de las herramientas, medios o dispositivos que permiten el tratamiento, creación y difusión de informaciones y comunicaciones de distinto tipo a escala planetaria, reclamando al derecho adecuarse a estos efectos para prevenir y regular las acciones de los usuarios y de quienes realizan transacciones de distinta naturaleza.

Cuando nos referimos a la protección de datos personales hablamos de crear elementos de prevención y regulación a partir de dos importantes factores de riesgo: la amenaza derivada del uso de las tecnologías de la información en perjuicio de la intimidad y privacidad de las personas por parte de terceras personas y de manera derivada, la probable afectación de los datos o uso ilícito de estos a partir de conductas lesivas ya sea por dolo o negligencia, de parte de los responsables de los archivos o registros públicos o privados.

Ahora bien ¿Por qué es importante la protección de datos personales? En primer término conviene definir algunos conceptos. Por *datos de carácter personal* debemos entender “toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona

física identificada o identificable”. Una gran parte de los datos de carácter personal pueden ser objeto de protección ante el riesgo de que afecten la intimidad o privacidad de las personas y con ello se vulneren por parte de terceros derechos fundamentales o esenciales para el bienestar del titular de los datos. Estos datos se refieren a los de origen étnico-racial, características físicas, morales o emocionales, vida familiar o afectiva, domicilio, número telefónico, patrimonio, ideología, opiniones políticas, afiliación gremial, creencias científicas, religiosas o filosóficas, preferencias sexuales, estado de salud físico o mental ,etc.

Mientras algunos datos deben ser especialmente protegidos, otros pueden ser publicables sin riesgo alguno para su titular. De esta manera, lo que se pretende proteger siempre es el dato de su titular como acción preventiva inicial ante el riesgo de ser tratado o elaborado y convertirlo en información, salvo para aquellos fines y por personas autorizadas para ello. De manera complementaria, el derecho objeto de su protección o el bien jurídico tutelado es el derecho a la intimidad y privacidad de las personas.

MARCO NORMATIVO GENERAL

En México existen referentes legales, jurisprudenciales y doctrinarios en materia de protección a la intimidad y privacidad de las personas en la Constitución General de la República, en Leyes Federales y en la legislación secundaria. En los artículos 7 y 16 de la Constitución General de la República se establecen criterios tutelares de la privacidad e intimidad de las personas. En el artículo 16 se regulan dos aspectos relevantes de la garantía protectora del Estado: la inviolabilidad domiciliaria y de las comunicaciones privadas.

Además de la Constitución General, en la legislación penal se encuentra regulada la *inviolabilidad domiciliaria* también conocida como la zona del retiro. Si bien, el domicilio es el espacio vital para que los individuos hagan uso de su núcleo familiar y de amistades para desenvolverse en la forma que les convenga, sin que existan intromisiones, ataques o manifestaciones de terceras personas públicas o privadas que transgredan los valores esenciales sobre los cuales se han fundamentado esas relaciones, encontramos que toda

intromisión al domicilio será ilícita cuando no hubiere consentimiento del titular o mandamiento de autoridad judicial, salvo en caso de flagrante delito ante un caso de robo o secuestro que ha sido al momento de su realización; o de hipótesis que generen causa de justificación, como puede ocurrir en el estado de necesidad, es decir, cuando se encuentren en grave peligro la integridad física o los bienes de quienes habitan ese domicilio, tal es el caso de un incendio, de un homicidio o intento de éste.

En lo referente a la *inviolabilidad de las comunicaciones*, también conocida como el secreto de la correspondencia o de las comunicaciones o la inviolabilidad de las cartas y otros papeles privados, encontramos dificultad para definir el derecho al secreto, habida cuenta de que existen formas diversas de vulneración e interceptación de comunicaciones e informaciones mediante vía telefónica, satelital, por comunicación escrita convencional y en Internet, donde abundan intromisiones de terceros a las comunicaciones privadas de los individuos vía correo electrónico. Sin embargo, la regulación en dicho artículo y la que existe en la legislación de acceso a la información pública vigente en el país no es suficiente para garantizar la *autodeterminación informativa* entendida como la posibilidad de control de parte del titular de la información de sus datos que obran en poder de archivos públicos. En esencia, se pretende con ello poner un límite a la acción intervencionista del Estado en cuanto a la invasión a la intimidad y privacidad de las personas.

El derecho a la propia imagen como parte de los derechos personalísimos se encuentra vinculado con el derecho a la privacidad consistente en “una garantía frente a la captación, reproducción, filmación o publicación por fotografía, filme o cualquier otro procedimiento de la imagen de una persona en lugares o momentos de su vida privada, así como la utilización del nombre, la voz o la imagen de una persona para fines publicitarios o comerciales”. Esta figura se encuentra poco regulada en México en el artículo 7 de la Constitución General de la República, en la Ley Federal de Derechos de Autor, en la legislación civil y penal.

La ambigüedad del término *daño moral* como sinónimo del derecho a la propia imagen en nuestra legislación queda fuera de duda cuando incluye el derecho a honor, intimidad y

propia imagen en la redacción del artículo 1916 del código civil del D. F. que señala: "...la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físico, o bien en la consideración que de si mismo tienen los demás". La lesión al *daño moral* busca la reparación al daño mediante una erogación material y carece de castigo con pena corporal y se diferencia de la *difamación y la calumnia* en que en estas se impone pena alternativa.

En el Código Penal Federal se protege otro aspecto importante de la intimidad: *el derecho al honor*. En términos generales este derecho puede asociarse a la buena reputación, al prestigio profesional e incluye la fama pública o buen nombre del que goza una persona. Los artículos 350 al 363 regulan el tema y se encuentra asociado a los delitos de difamación y calumnias. Las resoluciones de tribunales competentes han expresado el criterio de que este derecho debe preservarse después de muerta la persona y proceder a la reivindicación póstuma a partir de múltiples casos en que se han dado sentencias y acusaciones que en vida causaron grave daño a la reputación, dignidad y hasta la muerte.

Sin embargo, es a partir del año 2002 con la aprobación de la Ley de Acceso a la Información Pública del Estado de Sinaloa y la Ley Federal de Transparencia y Acceso a la Información Pública cuando se inicia de manera incipiente pero necesaria para el tratamiento del tema, con la incorporación de la figura del Hábeas Data como garantía procesal orientada a la protección de datos personales respectivamente, más tarde la mayoría de los estados incluirían en sus legislaciones esta figura conocida también como protección jurídica de datos personales por parte de la legislación Argentina aunque justo es decirlo, en la legislación Española se hace una interesante diferenciación entre el Hábeas Data y la protección jurídica de datos personales.

Como sabemos, en nuestro país, el Estado de Colima cuenta hasta hoy con la única Ley Estatal de Protección de Datos Personales aprobada por el Congreso del Estado, mientras que el IFAI cuenta con un capítulo en la LFTAIP sobre protección de datos personales y un reglamento que fija criterios importantes sobre el tema, previendo un organismo rector para dirimir conflictos. En nuestro Estado existe una iniciativa de Protección de Datos

Personales presentada a la soberanía del Congreso del Estado en el mes de junio de 2003 que no ha sido discutida y aprobada aún. De nuestra parte, consideramos que todavía quedan pendientes en la agenda nacional definir criterios sobre la pertinencia o no de la aprobación de parte del Congreso General de una Ley General de Archivos y otra Ley General de Protección de Datos Personales que regulen tanto a las entidades públicas y privadas para que sirvan como referente tanto a la legislación federal como a las legislaciones estatales.

Otros referentes normativos que dan protección a los datos personales son la Ley de Estadística y Geografía que prohíbe la publicación en una sola estadística de datos concernientes a personas físicas o morales. Contempla que los datos no deben asociarse a nadie y que los obtenidos con fines estadísticos carecen de validez legal. Por su parte la Ley de Salud pública regula como y quienes tienen acceso a los expedientes médicos de los ciudadanos. En el mes de enero de 2002, el Congreso de la Unión emitió una ley para normar a las Sociedades de Información Crediticia en donde se pretende regular los datos personales que manejan dichas entidades como son el Buró de Crédito y el sistema bancario.

EL IMPACTO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

Un aspecto relevante del tema en cuestión tiene que ver con la protección de los datos personales en Internet o en programas informáticos. Desde hace algún tiempo este campo de estudio le ha correspondido al derecho informático o al derecho de la informática, también incluye a la biotecnología, a la ingeniería genética, a la electrónica y a las telecomunicaciones en su espectro más amplio. A partir de las reformas al Código de Comercio, a la Ley Federal de Protección al Consumidor, Código Civil y Código de Procedimientos Civiles en nuestro país se regula el comercio electrónico. La novedosa forma de intercambio comercial por medios electrónicos, compras en Internet o intercambio de datos e información entre los usuarios, dan cuenta de la importancia de proteger los derechos de la privacidad e intimidad de las personas.

En la fracción I del artículo 76 bis de la Ley Federal de Protección al Consumidor se impone la obligación a los proveedores de mantener la confidencialidad de la información y la prohibición de difundirla o transmitirla a otros proveedores, a menos que el consumidor lo haya autorizado por escrito o que exista un requerimiento de alguna autoridad. La fracción II de este artículo obliga al proveedor de mantener segura y confidencial la información e informar al consumidor sobre las características generales de los elementos técnicos disponibles antes de la celebración de una transacción.

En el Código de Comercio, en el Código civil y de Procedimientos Civiles se regula el llamado “Mensaje de Datos Personales” a partir del auge de las Tecnologías de la Información. El “MDP” es considerado en el artículo 89 del Código de Comercio”. “En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denominará *mensaje de datos*”. A su vez, en el artículo 91 se establece “para efecto de éste Código de Comercio, se entiende por *sistema de información* cualquier medio tecnológico utilizado para operar mensajes de datos”. Es indudable que el Mensaje de Datos se encuentra relacionado con el intercambio de información económica o comercial a través de vía Telefónica, Fax, Radio, Televisión, Telégrafo, Satélite e Internet, contando con un mercado amplísimo para desarrollarse, estableciendo nuevas y dinámicas formas de hacer negocios, lo que requiere de mucho cuidado en el tratamiento de la información y comunicación, haciendo necesaria la protección del derecho a la privacidad de las personas.

Este fenómeno denominado e-commerce involucra tanto a personas físicas como jurídicas, al incluir entre éstas a los gobiernos federal, local y municipal, ha surgido lo que se ha dado en llamar el sistema del e-Gobierno, ya que a través de este se pretende garantizar a los ciudadanos el libre acceso a una gama de servicios públicos integrales, como los sistemas de información pública y trámites en línea ante las diversas dependencias de la administración pública federal, estatal y municipal. El manejo de información proveniente de los ciudadanos obliga a estas entidades a garantizar el derecho a la privacidad e intimidad de las personas.

Las Tecnologías de la Información también han traído conductas lesivas a la privacidad e intimidad sancionadas por la legislación penal. Estas conductas ilícitas son consideradas dentro de los delitos informáticos y se encuentran reguladas en el Código Penal Federal, Código Penal del Distrito Federal., Código Penal del Estado de Sinaloa , Ley Federal de Derechos de Autor y Ley de Protección de Datos Personales del Estado de Colima principalmente.

El artículo 167 fracción VI del Código Penal Federal sanciona a quien dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales por medio de las cuales se transmitan señales de audio, video o de datos. Aquí se incluye al interceptor de un correo antes de que llegue a su destino. La misma fracción VI sanciona la interceptación de datos que las personas envían a través de la red (sniffer). A su vez el artículo 211bis 1 al 211bis 7 del citado ordenamiento sanciona el acceso no autorizado a sistemas o servicios y destrucción de programas o datos en poder de instituciones del estado o del sistema financiero. Por su parte, en una redacción similar a la anterior, en el artículo 231 fracción XIV del Código Penal del Distrito Federal, se imponen sanciones a quienes cometan fraude mediante el uso de computadora y la manipulación de la información que estas contienen (técnica de salami y otras).

Al igual que en el Código Penal Federal, en el artículo 11 de la Ley Federal de Derechos de Autor ofrece sancionar la reproducción no autorizada de programas informáticos debido a que la reproducción queda protegida a favor del autor de las obras literarias o artísticas, entre las que se incluyen a los programas de cómputo. En los artículos 107 a 110 del mismo ordenamiento se sanciona el uso no autorizado de programas y bases de datos a menos que exista consentimiento del autor. La protección se otorga a datos que por su contenido sean obras intelectuales o información privada de las personas.

El Código Penal del Estado de Sinaloa contempla dentro del apartado correspondiente a los delitos patrimoniales, un capítulo denominado *Delito Informático* cuya redacción es la siguiente:

Art. 217: “Comete delito informático, la persona que dolosamente y sin derecho:

- I. Use o entre a una base de datos, sistema de cómputo o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información no como también:
- II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días de multa”.

Al margen del análisis de fondo que pueda darse al precepto en mención, importa destacar que en el citado precepto se recogen figuras lícitas que ya hemos comentado en la legislación penal federal y del Distrito Federal, tipificándose el fraude y las acciones intervencionistas en la intimidad y privacidad del titular de los datos.

La Ley de Protección de Datos del Estado de Colima amplía algunos de los criterios que se encuentran en la LFTAIP y su reglamento y la mayoría de las leyes de acceso a la información que se encuentran vigentes en el país. Conforme a esta, los principios bajo los cuales deben manejarse los datos personales comprenden: que sólo deben obtenerse y ser sujetos de tratamiento cuando sean adecuados, pertinentes y no excesivos, deben ser correctos y actualizados, deben obtenerse por medios lícitos y será necesario el consentimiento del interesado.

EL MARCO NORMATIVO LOCAL

El artículo 189 del Código Penal del Estado de Sinaloa señala que “*Al que mediante comunicación dolosa, impute a una persona física o moral un hecho que cause a esta*

descrédito, deshonra o afecte su reputación se le impondrá prisión de tres meses a dos años o de noventa a ciento ochenta días de multa". El precepto citado se refiere a la figura de la difamación en tanto que el 193 a la de la calumnia como parte de los delitos contra el honor al anotar que *"Al que impute falsamente a otro un hecho que la ley califique como delito, a sabiendas de que este no existe o de que el imputado no es responsable del mismo, se le impondrá prisión de seis meses a dos años o de noventa a ciento ochenta días de multa"*.

La Ley General de Salud del Estado de Sinaloa en su artículo 151 contempla que el registro estatal de donadores tiene carácter de *confidencial* teniendo acceso a su información: la autoridad judicial, la autoridad sanitaria, el Consejo Estatal de Transplantes y los establecimientos autorizados conforme a la ley, para la realización de transplantes, en los casos y con las limitaciones que establece este ordenamiento. Por su parte, el artículo 158 señala que el ejercicio de las profesiones de las actividades técnicas y auxiliares y de las especialidades para la salud, estará sujeto a las especificaciones que haga la Ley de Profesiones del Estado.

Por su parte, el artículo 181 establece una leve mención a la protección de los datos personales. Una polémica que debe ser resuelta es la que se refiere al criterio mantenido por las dependencias de salud –amparadas en la Norma Oficial Mexicana 168-, en el sentido de que los registros y archivos que obran en su poder le pertenecen a cada dependencia y no al titular de los datos, de manera que este sólo puede tener acceso a un resumen de su expediente clínico. Este tema ya ha sido materia de regulación en el IFAI, en la Red Iberoamericana de Datos Personales y en la legislación de muchos países.

En la Ley del Notariado del Estado de Sinaloa se encuentran algunos criterios protectores de la intimidad y privacidad de las personas. El artículo 17 obliga a los notarios a guardar debida reserva con respecto a la información confidencial de sus clientes y están sujetos a responsabilidad penal a partir de la violación del secreto profesional. El notario podrá ser suspendido hasta un año de su *fiat* si incurre en revelación dolosa e injustificada de datos de sus clientes y en caso de reincidencia, podrá haber separación definitiva y

consecuentemente, la revocación o cancelación del fiat. Pese a lo anterior, en esta etapa no puede hablarse de una protección jurídica de los datos personales, será la revolución de las tecnologías de la información y comunicaciones la que impulsará la necesidad de regular la protección de los datos personales.

En este contexto, el régimen de responsabilidad de los servidores públicos en materia de protección de datos personales se encuentra contemplado en la Ley de Responsabilidad de los Servidores Públicos del Estado de Sinaloa, comprende a aquellos que integran el poder ejecutivo, legislativo, judicial, entidades paraestatales, municipal y paramunicipales. El capítulo noveno de la Ley de Acceso a la Información Pública del Estado de Sinaloa se refiere a las faltas *administrativas y sanciones* que se aplicarán a los titulares de cada entidad pública, *en los términos y condiciones previstos por la Constitución Política del Estado de Sinaloa* por incumplir con lo estipulado en el artículo 9 de la LAIPES referente a la información mínima de oficio que las entidades deben otorgar al público, además este apartado hace suyas las obligaciones y sanciones establecidas en los artículos 47, 50 y 52 de la Ley de Responsabilidad de Servidores Públicos de nuestro Estado. Finalmente, es conveniente señalar que estas responsabilidades incluyen a los integrantes de organismos públicos autónomos como el Consejo Estatal Electoral, la Comisión Estatal de Derechos Humanos y la propia CEAIPES.

NECESIDAD DE UN MECANISMO DE PROTECCIÓN JURÍDICA EFECTIVO

La protección de los datos personales en la actualidad amerita un mecanismo de protección jurídica más amplio y efectivo, ya que el derecho a la privacidad e intimidad sustentado sobre los pilares que edifica el derecho fundamental de Hábeas Data se refiere a una parte, pero no a todo el marco protector de los datos personales. Debe tener como finalidad inicial el que cualquier persona pueda acceder a la información que sobre ella exista en cualquier registro o banco de datos. Para ello es preciso ejercitar un procedimiento especial relativo a la solicitud de información de datos personales, con plazos y términos bien definidos, en donde se hace preciso inicialmente estructurar esta solicitud en la entidad pública en donde se encuentren este tipo de información personal. Esta dependencia deberá recepcionar esta

solicitud e integrar un procedimiento administrativo en torno al mismo con el propósito fundamental de compartir con el solicitante los archivos que requiere. Lo anterior se fundamenta en el derecho que tiene todo titular de los datos a conocer el tipo y calidad de información que poseen y procesan cada una de las dependencias públicas. El único requisito de fondo que debe contemplar esta solicitud es la identificación plena del solicitante.

Un segundo momento procesal que habrá de contemplarse en este procedimiento se deriva de la posibilidad jurídica que tiene cualquier persona, titular de los datos personales de accionar en torno a la actualización, rectificación, supresión o modificación de los datos que consten en las Entidades Públicas relativos a su individualidad, para lo cual el detonante ante las dependencias sería la manifestación expresa de la voluntad del sujeto tendiente a realizar la transformación de la información y los elementos probatorios que la persona pueda aportar para comprobar de la forma más clara posible la base jurídica que sostenga su afirmación.

Ambos momentos procesales deberán tener términos breves y precisos y que contribuyan a garantizar la protección integral de este derecho fundamental. Aunado a esto se requiere la vigilancia y tutela de un órgano especializado en los procesos de información y que se constituya como la garantía procesal que proteja la identidad, la privacidad, la intimidad y la autodeterminación informativa que cada persona debe ejercitar. El titular de los datos podrá exigir en todo momento y sin plazos perentorios que los sujetos obligados que administren, manejen, archiven, posean y conserven en su poder información confidencial en bases de datos, archivos o registros públicos, garanticen un adecuado uso y tratamiento de los datos sensibles.

CONCLUSIONES

En México, los antecedentes para una protección de datos personales se inician con el marco constitucional y de leyes federal y estatal en materia de protección a la privacidad e

intimidad de las personas, pero la aparición de las nuevas tecnologías de la información y comunicaciones han sido determinantes para la existencia de un incipiente marco regulador en materia de datos personales, primero con la ley de geografía y estadística, con la legislación bursátil, con la de salud, y telecomunicaciones. Más recientemente, con las de transparencia y acceso a la información, la de protección de datos personales del Estado de Colima y la reglamentación del IFAI.

Las transformaciones que ha experimentado la sociedad en los tiempos contemporáneos hacen necesarias medidas de protección y regulación que impregnen de seguridad y certeza jurídica a los datos de carácter personal que se encuentran bajo el resguardo de instituciones públicas y privadas. Esta problemática se estructura bajo un dualismo: Inicialmente por la relativa facilidad que los medios electrónicos y la sistematización de la información tienen para ser vulnerados y obtener por esos conductos información de carácter personal, y en un segundo momento por la tendencia de los funcionarios que manejan esta información en otros formatos que permiten que esta información se haga del conocimiento público.

La protección de los datos personales constituye una prioridad jurídica estructurada inicialmente bajo la conceptualización de un derecho fundamental denominado Hábeas Data, que funciona para que no se comparta la información íntima y para que esta información pueda corregirse, actualizarse o modificarse en todo momento, acción que se puede intentar solamente por su titular. En nuestro país se requiere intensificar la protección jurídica en torno a los datos personales, bajo mecanismos que van desde la protección legal en los procesos de captación, almacenamiento, sistematización y modos de compartirla, hasta los mecanismos legales para conocer datos propios y modificarlos cuando son imprecisos o erróneos. Algunos aspectos normativos actuales se relacionan con la intimidad y complementan su noción protectora, entre ellos destacan la inviolabilidad domiciliaria, la inviolabilidad de comunicaciones y el derecho a la propia imagen, cada uno de ellos estructura sus propios bienes jurídicos tutelados y la forma de ejercitarlos. Las nuevas tecnologías de la información también inciden en el tema de protección de datos personales, principalmente en torno al tema de mantener segura la información personal sistematizada.

Ello ha obligado al avance normativo en torno a materias como contratos informáticos o electrónicos, flujo de datos transfronterizos, comercio electrónico, gobierno electrónico y delitos informáticos.

Resulta necesario implementar un mecanismo de protección jurídica en torno a los datos personales, bajo un procedimiento que asegure su ejercicio y que permita acceder a la información personal de la que cada individuo es titular y que además asegure la forma jurídica para cambiarla cuando así se requiera.

Vicente Hernández Delgado

Estudios Profesionales en la Escuela Superior de Derecho de la Universidad Autónoma de Nayarit y en la Escuela de Ciencias Sociales de la Universidad Autónoma de Sinaloa Zona Sur Mazatlán. Postgrado: “Especialidad en Microcomputadoras”, proyecto auspiciado por la coordinación académica de la zona sur, Mazatlán, “Master Internacional en Derecho Penal, Constitución y Derechos”, proyecto impulsado por la Universidad Autónoma de Barcelona, Universidad Autónoma Metropolitana y la Universidad Autónoma de Sinaloa. **Comisionado de la Comisión Estatal para el Acceso a la Información Pública del Estado de Sinaloa.**