OFICINA DEL ALTO COMISIONADO PARA LOS DERECHOS HUMANOS

08/2018

PRINCIPIOS Y BUENAS PRÁCTICAS IMPLEMENTADAS EN MÉXICO

EN TORNO AL DERECHO A LA PRIVACIDAD

INFORME DEL ESTADO MEXICANO EN RESPUESTA A LA SOLICITUD DE INFORMACIÓN DE LA OFICINA DEL ALTO COMISIONADO SOBRE EL DERECHO A LA PRIVACIDAD,

DEL 8 DE MARZO DE 2018.

Ciudad de México, 9 de abril del 2018.

ÍNDICE

PRINCIPIOS Y BUENAS PRÁCTICAS INSTRUMENTADAS EN MÉXICO EN TORNO AL DERECHO A LA PRIVACIDAD

A. AVANCES LEGISLATIVOS A NIVEL LOCAL Y FEDERAL EN MATERIA DE PRIVACIDAD EN LA ERA DIGITAL.

1. Derivado del desarrollo de las tecnologías de la información, en la actualidad es posible almacenar un número ilimitado de datos e información relativa a las personas físicas identificadas o identificables y utilizarlos para fines indistintos, los cuales pueden circular en cuestión de segundos entre países, empresas privadas y redes abiertas.

2. El despliegue de tecnología trajo consigo el reconocimiento de un nuevo derecho fundamental: el derecho a la protección de datos personales, el cual fue equiparado en sus orígenes con el derecho a la intimidad o privacidad; sin embargo, la concepción tradicional del derecho a la intimidad no ofrecía una garantía suficiente y vasta cuando se trataba de la explotación, manejo, análisis, circulación, almacenamiento y uso indiscriminado de datos personales en manos de terceros.

3. En consecuencia, fue necesario reconocer el poder de disposición, que implica decidir, quién, cómo, cuándo y para qué se utilizarán los datos personales. De esta manera, se hizo patente la necesidad de adoptar instrumentos regulatorios que garantizaran, por una parte, la protección de las personas físicas con relación al tratamiento de sus datos personales y, por la otra, el libre flujo de los datos personales que actualmente constituyen la base para el desarrollo, fortalecimiento e intercambio de bienes y servicios en una economía global y digital, sobre los cuales se erigen la economía de cualquier país.

4. El Estado mexicano reconoce la importancia de establecer reglas tendientes a procurar que los datos personales sean utilizados adecuadamente, tanto por el Estado como por el sector privado, a efecto de salvaguardar el derecho a la protección de los datos personales.

5. El primer instrumento normativo en materia de protección de datos personales en México es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en 2002 y en cuyo capítulo IV se establecieron los principios generales que deben regir el tratamiento de datos personales en posesión de los entes públicos, del orden federal, así como disposiciones generales que daban vida a los derechos de acceso y rectificación.

6. En 2009, el derecho a la protección de datos personales se incorporó al listado de derechos fundamentales reconocidos a nivel constitucional; específicamente en el artículo 16, segundo párrafo; en 2010, se publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

7. El 2014, la reforma al artículo 6 constitucional fijó las bases para la emisión de una ley general que permitiera dimensionar la extensión del derecho a la protección de datos personales, entre todos los entes públicos de los tres órdenes de gobierno y la sociedad mexicana.

8. En 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante, Ley General); es el primer ordenamiento mexicano que, a nivel nacional, establece las bases y los estándares mínimos e imprescindibles que permiten uniformar el derecho a la protección de datos personales en el país en el sector público federal, estatal y municipal.

9. La Ley General es aplicable a todos los entes públicos federales y partidos políticos nacionales y los Congresos estatales contaron con un plazo máximo de seis meses, contados a partir de la entrada en vigor de la Ley General, para efectuar las adecuaciones normativas correspondientes a su legislación existente en la materia, a fin de que ésta respondiera a los nuevos estándares señalados en la Ley General. Actualmente, treinta entidades federativas han publicado legislación en la materia.

10. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Sistema Nacional de Transparencia), publicaron los siguientes instrumentos secundarios en el ámbito de sus respectivas atribuciones y competencias a fin de hacer exigibles las obligaciones contenidas en la Ley General:

- Lineamientos Generales de Protección de Datos Personales para el Sector Público, aplicables al sector público federal.
- Lineamientos Generales para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ejerza la facultad de atracción.
- Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, aplicables a los tres órdenes de gobierno.
- Criterios generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal, aplicables a los tres órdenes de gobierno.
- Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, aplicables a los tres órdenes de gobierno.

11. El Estado mexicano destaca la importancia del Programa Nacional de Protección de Datos Personales (Pronadatos), considerado como un elemento innovador en el marco de la Ley General. El Pronadatos es el primer instrumento en el país que define la política pública respecto al derecho a la protección de datos personales, bajo los siguientes ejes:

- La consolidación de una cultura de protección de datos personales entre la sociedad mexicana;
- El fomento del ejercicio del derecho a la protección de datos personales;
- La capacitación de los servidores públicos de los tres órdenes de gobierno; y
- La medición, reporte y verificación de las metas establecidas en el Programa.

Reglas generales aplicables a los tratamientos de datos personales que se efectúen en el ámbito federal

12. A nivel federal, el derecho a la protección de datos personales se regula a través de dos instrumentos: la Ley General y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley Federal) y son administradas por una sola autoridad garante: el INAI. Así, de manera específica el sector público federal es regulado por la Ley General, los Lineamientos Generales y demás legislación secundaria; en tanto que las actividades del sector privado son reguladas por la Ley Federal, su Reglamento y demás normatividad derivada.

B. JURISPRUDENCIA EN MATERIA DEL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL

13. El Estado mexicano informa que el Poder Judicial de la Federación, mediante sus decisiones ha reafirmado la importancia del derecho a la privacidad. Así, ha dispuesto que todas las formas existentes de comunicación incluidas aquéllas que sean resultado del desarrollo tecnológico, deben ser protegidas por el derecho fundamental a la inviolabilidad de las comunicaciones privadas.

14. Asimismo, la protección de los datos personales de las personas físicas e información de las personas jurídicas ha sido motivo de atención del Poder Judicial, en aquellos supuestos en los que de revelarse, podría generar afectaciones en contra de sus titulares.

15. Las resoluciones del Poder Judicial han reconocido que la intimidad como derecho humano tiene distintos niveles de protección, en función del carácter del Estado; es decir, si éste se constituye como garante o protector frente a la sociedad o ante su propia actividad. Adicionalmente, la inviolabilidad del domicilio ha sido objeto de análisis del Poder Judicial, el cual lo considera un espacio de acceso reservado

en el cual los individuos ejercen su libertad en la esfera más íntima y cuya protección prevalece con independencia de cualquier consideración material.

16. A continuación se presenta una selección de las decisiones más relevantes de la Suprema Corte de Justicia de la Nación (SCJN) y los Tribunales Colegiados de Circuito (TCC) en materia de derecho a la privacidad:

i. Derecho a la inviolabilidad de las comunicaciones privadas. Su objeto de protección incluye los datos que identifican a la comunicación.[1]

ii. Derecho a la inviolabilidad de las comunicaciones privadas. Momento en el cual se considera interceptado un correo electrónico. Se entenderá que un correo ha sido interceptado cuando –sin autorización judicial o del titular de la cuenta-, se ha violado el *password* o clave de seguridad. En ese momento y sin necesidad de analizar el contenido de los correos electrónicos, se consuma la violación al derecho fundamental a la inviolabilidad de las comunicaciones privadas[2].

iii. Flujo de información en red electrónica (internet).Principio de restricción mínima posible. Atento a la importancia de las nuevas tecnologías de la información y la comunicación que permiten la existencia de una red mundial en la que pueden intercambiarse ideas y opiniones, conforme al criterio del Comité de Derechos Humanos de la ONU; el Estado debe adoptar todas las medidas necesarias a fin de fomentar la independencia de los nuevos medios y asegurar a los particulares el acceso a éstos. Lo anterior, en función de que el internet se ha constituido como un medio fundamental para que las personas ejerzan su derecho a la libertad de opinión y de expresión; gracias a sus características singulares tales como, su velocidad, alcance mundial y relativa anonimidad. Por tanto, se reconoce que el orden jurídico nacional y en el derecho internacional de los derechos humanos existe un principio a la mínima restricción posible del flujo de información en internet[3].

iv. Libertad de expresión y opinión ejercidas a través de la red electrónica (internet) Restricciones permisibles. A fin de que las limitaciones puedan considerarse apegadas al parámetro de regularidad constitucional, resulta indispensable que éstas se encuentren previstas por ley, se basen un fin legítimo y sean necesarias así como proporcionales. Adicionalmente, debe precisarse que la relación entre el derecho

[1] Novena Época. Registro: 161335; Instancia: Primera Sala; Tesis Aislada.
[2] Novena Época. Registro: 161339; Instancia: Primera Sala; Tesis Aislada.
[3] Décima Época. Registro: 2014515; Instancia: Segunda Sala; Tesis Aislada.

y la restricción no debe invertirse; esto es, la regla general es la permisión de la difusión de ideas, opiniones e información y excepcionalmente, el ejercicio del derecho puede restringirse[4].

v. Información pública. Es aquélla que se encuentra en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal; siempre que se haya obtenido por causa del ejercicio de funciones de derecho público. Los poderes públicos no están autorizados para mantener secretos y reservas frente a los ciudadanos en el ejercicio de las funciones estatales que están llamados a cumplir, salvo las excepciones previstas en la ley, que operan cuando la revelación de datos puede afectar la intimidad, la privacidad y la seguridad de las personas. En ese orden de ideas, la información pública es el conjunto de datos de autoridades o particulares en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal; obtenidos por causa del ejercicio de funciones de derecho público[5].

C. MARCO JURÍDICO APLICABLE EN MATERIA DE RECOLECCIÓN, PROCESAMIENTO Y RESGUARDO DE DATOS PERSONALES EN MANOS DE GOBIERNOS Y OTROS ACTORES, TALES COMO EMPRESAS.

17. A continuación se señalan las principales obligaciones que las personas físicas o morales de carácter privado deben observar en todos los tratamientos de datos personales, en términos del marco jurídico aplicable:

i. Relacionadas con el tratamiento de datos personales

- Tratar los datos personales con apego y cumplimiento de lo dispuesto por la legislación mexicana y el derecho internacional que le resulte aplicable al responsable de carácter privado;
- No utilizar medios engañosos o fraudulentos para obtener los datos personales;
- Tratar los datos personales privilegiando la protección de los intereses del titular y su expectativa razonable de privacidad;
- Recabar el consentimiento, libre, específico e informado, del titular para el tratamiento de sus datos personales, ya sea en su modalidad tácita o expresa según corresponda;
- El consentimiento tácito será aplicable cuando se utilicen datos personales que no estén catalogados como sensibles, patrimoniales o financieros y se perfecciona cuando se pone a disposición del titular el aviso de privacidad sin que éste manifieste oposición alguna al respecto.
- El consentimiento expreso es aplicable cuando lo exija una disposición legal o reglamentaria; se utilicen datos personales financieros patrimoniales o sensibles; lo solicite el responsable de carácter privado para acreditar su obtención, o bien, cuando el titular o el responsable de carácter privado de común acuerdo decidan plasmar de esa forma el consentimiento, sin que exista obligación legal. Se

[4] Décima Época. Registro: 2014519; Instancia: Segunda Sala; Tesis Aislada.
[5] Novena Época. Registro: 164032; Instancia: Segunda Sala; Tesis Aislada.

perfecciona cuando la voluntad del titular se manifiesta de forma verbal, escrita, medios electrónicos, ópticos, signos inequívocos o cualquier otra tecnología. Por regla general, es válido el consentimiento tácito para cualquier tratamiento de datos personales.

- Procurar que los datos personales sean correctos y actualizados para los fines que fueron recabados.
- Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad.
- Definir el periodo de conservación de los datos personales, tomando en cuenta los valores administrativos, contables, fiscales, jurídicos e históricos de los datos personales.
- Analizar las finalidades que justifican el tratamiento de los datos personales, a efecto de disponer de la mínima cantidad de éstos para conseguir el objetivo perseguido, poniendo especial atención en datos personales sensibles.
- Adoptar las medidas necesarias que permitan al responsable de carácter privado acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley Federal y demás normatividad aplicable.
- Informar al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a través del aviso de privacidad, el cual tiene por objeto delimitar los alcances y condiciones generales del tratamiento de éstos.
- Poner a disposición del titular el aviso de privacidad, en sus tres modalidades: integral, simplificado y corto.

ii. Relacionadas con la implementación de medidas de seguridad

- Establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales tratados contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
- Determinar y establecer las medidas de seguridad que resulten aplicables a los datos personales en función de una serie de factores como son:
  a) El riesgo inherente por tipo de dato personal.
  b) La sensibilidad de los datos personales tratados.
  c) El desarrollo tecnológico.
  d) Las posibles consecuencias de una vulneración para los titulares.
  e) El número de titulares.
  f) Las vulnerabilidades previas ocurridas en los sistemas de tratamiento.
  g) El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
  h) Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable de carácter privado.
- Establecer y mantener una serie de acciones orientadas a garantizar la seguridad de los datos personales como son elaborar un inventario de los datos personales; elaborar un análisis de riesgos y de brecha; llevar a cabo revisiones o auditorías; capacitar al personal que efectúe tratamientos de datos personales, entre otras.

ii. Relacionadas con las vulneraciones de seguridad de datos personales que, en su caso, ocurrieran

- Informar al titular sobre las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirmara que ocurrió la vulneración que refiere y hubiere tomado acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación.
- La notificación al titular deberá señalar lo siguiente:
  a) La naturaleza del incidente, es decir, robo, pérdida, acceso o transferencias no autorizadas de datos personales, entre otros.
  b) Los datos personales comprometidos.
  c) Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.
  d) Las acciones correctivas realizadas de forma inmediata.
  e) Los medios donde puede obtener mayor información al respecto.
- Analizar las causas por las cuales se presentó la vulneración de seguridad e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.

iii. Relacionadas con la contratación de prestadores de servicios que, en su caso, se realice y en la cual se involucre el tratamiento de datos personales

- En términos de la Ley Federal, se denomina a los prestadores de servicios como "encargados" y éstos pueden ser una persona física o jurídica, de carácter público o privado, ajenos a la organización del responsable de carácter privado, que a solas o conjuntamente con otras, trata datos personales a nombre y por cuenta de éste.
- El encargado se encuentra obligado a:
  a) Tratar únicamente los datos personales conforme a las instrucciones del responsable de carácter privado.
  b) Abstenerse de tratar los datos personales para finalidades distintas a las instruidas el responsable de carácter privado.
  c) Implementar las medidas de seguridad conforme a la Ley Federal, el Reglamento y las demás disposiciones aplicables.
  d) Guardar confidencialidad respecto de los datos personales tratados.
  e) Suprimir los datos personales, objeto de tratamiento, una vez cumplida la relación jurídica con el responsable de carácter privado o por instrucciones de ésta, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
  f) Abstenerse de transferir los datos personales, salvo en el caso de que el responsable de carácter privado así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.
  g) Aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley Federal, su Reglamento y demás normativa aplicable.
  h) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.
  i) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de los datos personales sobre los que preste el servicio.
  j) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

iv. Relacionadas con la transferencia de datos personales

- La Ley Federal señala que una transferencia es toda comunicación de datos personales, de carácter nacional o internacional, realizada a persona distinta del responsable de carácter privado o del encargado.
- En caso de que un responsable de carácter privado decidiera realizar transferencias de los datos personales, ya sean nacionales o internacionales, estaría obligado a cumplir con lo siguiente:
  a) Obtener el consentimiento del titular para la transferencia de sus datos personales, sea nacional o internacional. Salvo que se actualice alguna de las siguientes excepciones:
  * Cuando la transferencia esté prevista en una ley o tratado en los que México sea parte.
  * Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.
  * Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable de carácter privado, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable de carácter privado que opere bajo los mismos procesos y políticas internas.
  * Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable de carácter privado y un tercero.
  * Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia.
  * Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
  * Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable de carácter privado y el titular.

D. ACCIONES TENDIENTES A PROTEGER ADECUADAMENTE EL DERECHO A LA PRIVACIDAD FRENTE A LAS AMENAZAS CREADAS POR EL USO DE LAS NUEVAS TECNOLOGÍAS:

18. México reconoce que las nuevas tecnologías basadas en la información permiten una mayor difusión en el intercambio de información, el ejercicio de derechos y libertades, el impulso de negocios, el fomento de la innovación y la libre expresión de las ideas. Su uso y la comunicación a través de ellas, puede favorecer el desarrollo de individuos, organizaciones y naciones por lo que debe ser utilizado de buena fe. Sin embargo, ni las nuevas tecnologías basadas en información y compilación de datos biométricos ni el ciberespacio se encuentran exentas de ser empleadas con fines maliciosos. Por ello, tanto la comunidad internacional como todos los actores involucrados deben unir esfuerzos para garantizar un ciberespacio libre y abierto, neutral y resiliente, y al mismo tiempo confiable y seguro, generando oportunidades que potencialicen el desarrollo de las personas y las comunidades, así como medidas para desincentivar y prevenir el uso negativo de estas herramientas.

19. Por lo anterior se ha puesto en marcha la Estrategia Nacional de Ciberseguridad, diseñada como un documento vivo, que establece la visión, objetivos y ejes y objetivos estratégicos para alcanzar un ciberespacio confiable, seguro y estable en la que se mantiene el firme compromiso para el desarrollar, junto con los tomadores de decisiones y otros actores interesados, estrategias para la privacidad y protección de datos enfatizando la transparencia en el sector público. Dicho documento se elaboró a partir de la colaboración entre instituciones de gobierno, organizaciones empresariales, de la sociedad civil y de los sectores técnico y académico, a través de talleres de discusión. Contó además con el acompañamiento técnico del programa de seguridad cibernética de la Organización de Estados Americanos, que permitió integrar la opinión de expertos internacionales y de la sociedad civil.

20. La Estrategia Digital Nacional que ha contribuido a maximizar la digitalización de los sectores público y privado, y maximizar el impacto que las tecnologías de la información y las telecomunicaciones tienen sobre el desarrollo económico, social y político de las personas. Con este marco institucional, México reitera su disposición de participar activamente en las deliberaciones internacionales que conduzcan a consolidar un uso legítimo y pacífico de las nuevas tecnologías como detonadoras del desarrollo inclusivo, sostenible y garantía de los derechos de las personas, a través del acceso y usos pacíficos de las mismas y de la libre difusión de las ideas, el ejercicio y protección de los Derechos Humanos en la red.

E. ACCIÓN DE LA COMUNIDAD INTERNACIONAL, INCLUIDA LA ONU, ANTE LOS DESAFÍOS EN MATERIA DE DERECHOS HUMANOS EN EL CONTEXTO DEL DESARROLLO TECNOLÓGICO DINÁMICO

21. A fin de reiterar su compromiso con la política internacional en materia de derechos humanos, el Estado mexicano ha promovido desde 2009, junto con otros países interesados, la resolución sobre "Acceso a la información pública" en el marco de la Asamblea General de la OEA. A raíz de dicha resolución, fue adoptada la Ley Modelo Interamericana sobre Acceso a la Información Pública en junio de 2010 y, subsecuentemente, en 2011 y 2013 se adoptaron resoluciones sobre "Acceso a la información pública y protección de datos."

22. En 2016 se adoptó una resolución tendiente a implementar el "Programa Interamericano sobre Acceso a la Información Pública" que busca avanzar en la adopción e implementación de legislación interna sobre acceso a la información pública.

23. México también ha promovido la inclusión de referencias a la transparencia y el acceso a la información en diversas resoluciones adoptadas en el marco del Consejo de Derechos Humanos y la Asamblea General, como en la resolución sobre "Libertad de opinión y expresión", "La función de la buena gestión pública en la promoción y protección de los derechos humanos", "El derecho a la privacidad en la era digital", "El espacio de la sociedad civil" y "La participación equitativa en asuntos públicos y políticos."

F. PRINCIPALES DESAFÍOS EN EL MARCO DEL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL, EN EL CONTEXTO DE GRUPOS EN SITUACIÓN DE VULNERABILIDAD.

24. El Estado mexicano enfrenta el reto de capacitar a todas y todos los servidores públicos en materia de protección de datos personales, para que cuenten con herramientas que les permitan atender los casos en la materia.

25. Otro desafío importante es el tratamiento de los datos personales de las personas privadas de la libertad. Actualmente, a través de la Comisión Nacional de Seguridad se encuentra en proceso de trasladar la información de la población penitenciaria al sistema denominado Sistema Integral de Centros Federales, el cual permita administrar una base de datos compatible con el Registro Nacional Penitenciaria y la Plataforma México. Lo anterior, a fin de evitar que la información de la población penitenciaria sea empleada con fines maliciosos.

G. MEDIDAS Y BUENAS PRÁCTICAS IMPLEMENTADAS A FIN DE PROTEGER A LOS GRUPOS EN SITUACIÓN DE VULNERABILIDAD.

26. A fin de proteger a los grupos en situación de vulnerabilidad en el contexto de la era digital, el Estado mexicano ha impartido cursos en línea para sensibilizar a las y los servidores públicos en materia de protección y resguardo de datos personales, así como sujetos obligados.

27. Asimismo, se encuentran disponibles los avisos de privacidad integrales en los portales de internet de todas las dependencia de gobierno, a fin de que la sociedad interesada pueda consultarlo si resulta de su interés.

28. También se brinda atención y asesoría en materia de datos personales a través de las Unidades Administrativas correspondientes y los Módulos de Información al público en general, en todas las dependencias gubernamentales, las cuales se encuentran habilitadas para recibir las solicitudes de información pública.

29. México reafirma su disposición plena para continuar implementando las acciones tendientes a fortalecer una política de promoción y defensa de los derechos humanos involucrados en el marco de la privacidad en la era digital, a través de una estructura institucional sólida y en cooperación con los principales organismos internacionales en la materia.