El Instituto Federal de Acceso a la Información Pública como órgano garante en materia de protección de los datos personales[1]

*Jacqueline Peschard Mariscal**

Introducción

En México, el Instituto Federal de Acceso a la Información Pública (en adelante IFAI)[2], es la autoridad especializada en materia de acceso a la información pública gubernamental y garante de la protección de los datos personales en posesión de las dependencias y entidades de la Administración Pública Federal, en lo sucesivo, Poder Ejecutivo Federal.

La prioridad para los Comisionados del IFAI en el arranque de la Ley Federal de Trasparencia y Acceso a la Información Pública Gubernamental[3] (la Ley) fue privilegiar la difusión del derecho a saber de todas las personas acerca de cómo hacen las cosas los órganos gubernamentales, cómo ejercen el gasto público, y cómo cumplen sus metas y los objetivos, entre otros muchos aspectos.[4]

Sin embargo, con el paso del tiempo y la especialización que fue dándose al interior de la Institución, la faceta de autoridad garante de la protección de los datos personales contenidos en los ficheros públicos (denominados por nuestra normativa como sistemas de datos personales) comenzó a desarrollarse, si bien, el ejercicio de los derechos de acceso y rectificación de datos fue plenamente observado desde el inicio por los entes gubernativos.

El presente artículo tiene como objetivo compartir las experiencias surgidas de las primeras verificaciones que se han efectuado a los sistemas de datos personales en posesión de la Administración Pública Federal, para conocer el grado de observancia del Capítulo IV, del Título Primero de la Ley de Transparencia, así como de los Lineamientos de protección de datos personales.[5]

---

*Doctora en Ciencias Sociales, por el Colegio de Michoacán. Miembro del Sistema Nacional de Investigadores y de la Academia Mexicana de Ciencias. Actualmente es Comisionada Presidenta del Instituto Federal de Acceso a la Información Pública (IFAI).

Verificaciones a sistemas de datos personales.

El objetivo de las verificaciones es conocer el cumplimiento que el Ejecutivo Federal da a los principios de protección de datos personales y evaluar las acciones implementadas, así como el nivel de observancia de la normatividad aplicable en esta materia, para la posterior emisión de recomendaciones.

En este sentido, a partir de 2007 se dio inicio a los procedimientos de verificación de sistemas de datos personales, a través de la notificación de requerimientos de información a distintas dependencias y entidades (seleccionadas previamente en razón de la importancia de los sistemas o la sensibilidad de los datos, entre otros criterios).

Los cuestionamientos específicos a las distintas instituciones abarcan los siguientes aspectos:

Cumplimiento de los principios de protección relativos a licitud, calidad, información, custodia y cuidado y seguridad;

Los procedimientos implementados por parte de las dependencias y entidades de la Administración Pública Federal para garantizar el ejercicio de los derechos de acceso y corrección (rectificación);6

El tratamiento y acciones realizadas al efectuar transmisiones de datos personales con dependencias, entidades o entes públicos federales, ya sea estatales o municipales; o bien con gobiernos u organismos internacionales;

Las medidas de seguridad administrativa, física y técnica, implementadas por el Ejecutivo Federal para asegurar la integridad, disponibilidad y confidencialidad de los datos personales en su posesión;

El registro de los sistemas de datos (registro de ficheros) en la herramienta generada para tal efecto, y

Los mecanismos para la contratación de los servicios de un tercero para el tratamiento de los sistemas de datos personales.

Durante el proceso de respuesta y envío de información al IFAI, se sostienen reuniones de trabajo con las distintas dependencias y entidades verificadas, lo cual permite, por una parte, sensibilizar a los responsables de los sistemas en cuanto al tratamiento de los datos y, por otra, contar con mayores elementos para emitir recomendaciones específicas, en razón de las respuestas proporcionadas por las unidades administrativas responsables del sistema objeto de verificación.

Emisión de Recomendaciones a sistemas de datos personales.

La recomendaciones se emiten mediante acuerdos tomados por mayoría de votos de los 5 comisionados que integran el Pleno del IFAI, las cuales tienen por objeto indicar ac-

ciones concretas para la debida observancia de los principios y derechos en materia de protección de datos personales, a partir de la identificación de las condiciones o puntos críticos detectados en las verificaciones realizadas, tales como riesgos existentes o potenciales, a efecto de minimizarlos. También el Instituto reconoce los avances registrados en el cumplimiento de la legislación y regulación secundaria por parte del Ejecutivo Federal.

A la fecha, el IFAI han emitido 62 recomendaciones en materia de protección de datos personales. Así, la tarea del IFAI en materia de protección de datos personales se ha centrado en construir una política pública de respeto y adecuado tratamiento a la información de las personas, a partir de dar a conocer los criterios del Instituto en cada caso concreto.

Los sistemas de datos personales verificados refieren a diversas finalidades, las cuales se encuentran vinculadas con las facultades y atribuciones lícitas y legales que cada órgano gubernamental tiene conferidas; finalidades que pueden comprender, solo por mencionar algunas, el control de programas sociales; registros de población; actividades de control migratorio; atención médica (expedientes clínicos); líneas de atención telefónica a víctimas de violencia; sistemas o ficheros de datos de control de personal con fines puramente administrativos, tales como los expedientes de personal, entre otros.

De esta suerte, los aspectos de interés que destacaron en el desarrollo de las verificaciones, fueron tan bastos como los ficheros en sí. En este sentido, por obvio de espacio, nos centraremos en algunos aspectos relevantes de las recomendaciones emitidas, tomando en cuenta la finalidad del sistema y la dependencia o entidad que los posee.

En principio, vale la pena referirnos a los sistemas de datos en posesión del Instituto Nacional de Migración,7 órgano técnico desconcentrado de la Secretaría de Gobernación, el cual tiene por objeto la planeación, ejecución, control, supervisión y evaluación de los servicios migratorios en el país, así como el ejercicio de la coordinación con las diversas dependencias y entidades de la Administración Pública Federal que concurren en la atención y solución de los asuntos relacionados con la materia migratoria.

Del análisis realizado a los sistemas de datos, FM1 Delegaciones, FM1 Electrónica, Sistema Integral de Operación Migratoria SIOM y LASERFICHE (Digitalización del Archivo Migratorio Central), entre otros, respecto al tratamiento de los datos de carácter personal por parte de las unidades administrativas responsables, arrojó en su generalidad resultados favorables. Por lo anterior, el IFAI realizó una serie de recomendaciones tendientes a mejorar, y en su caso, reforzar las medidas implementadas por el Instituto Nacional de Migración, tales como:

Incorporar en sus mecanismos escritos de recolección de datos la leyenda de información -aviso de privacidad- a que hace alusión el Decimoctavo de los Lineamientos de Protección de Datos Personales;

Definir y delimitar las atribuciones, funciones y obligaciones de los servidores públicos que interactúan con los datos personales, en el ejercicio de sus funciones, con el carácter de encargados y usuarios, y

Diseñar e instrumentar planes de capacitación que estén enfocados a difundir la normatividad aplicable en materia de protección de datos personales y las medidas de seguridad de índole administrativa, física y técnica implementadas para la adecuada protección de los datos personales contenidos en los sistemas, entre otras.

Cabe señalar, que el estudio realizado fue respecto de los datos personales que recaba el órgano desconcentrado en ejercicio de sus facultades de carácter administrativo, y no así para aquella información que le es proporcionada por los órganos de inteligencia y procuración de justicia del país en términos de lo señalado en los artículos 72 y 73 de la Ley General de Población,8 y 202 de su Reglamento.9

Ahora bien, por lo que hace a los ficheros relacionados con asistencia social, el sistema de datos personales denominado "Sistema de Acreditación de Derechohabiente" en posesión del Instituto Mexicano del Seguro Social10, se considera de gran relevancia, al tener como finalidad el registrar los datos de identificación de los derechohabientes del Instituto Mexicano del Seguro Social, para la expedición de un medio de identificación que simplifique la entrega de las prestaciones en especie y en dinero, a través de medios electrónicos modernos, eficaces y seguros que vincule al derechohabiente de forma única, confiable e inequívoca a las prestaciones a que tiene derecho.

Uno de los aspectos que merece mención de la verificación a dicho sistema, refiere a la contratación de los servicios de un tercero para el tratamiento de datos personales. El IFAI, pudo constatar que el Instituto Mexicano del Seguro Social cumple adecuadamente respecto a este rubro, al establece mediante un instrumento jurídico adecuado -un contrato- las acciones sobre tratamiento y seguridad que debe adoptar el prestador del servicio, a través de un clausulado específico, en el cual se exigen los siguientes puntos:

Los criterios de seguridad de la información que debe cumplir el proveedor en los que se incluyen integridad, confidencialidad, autenticación, control de accesos, no repudio, disponibilidad, auditoría y monitoreo, y

El destino final de los datos obtenidos como parte del proceso de enrolamiento, en el cual se establece que son propiedad de Instituto, y el proveedor es responsable de brindar el servicio de generación y entrega del documento de acreditación, así como la inserción del registro a la base de datos.

Como se desprende, numerosos son los aspectos positivos resultado de las recomendaciones emitidas por el Pleno del IFAI en materia de protección de datos personales; en particular, el IFAI ha sido contundente al indicar el tipo de medidas de seguridad que

impidan que los datos recabados sean sustraídos y utilizados para otros fines.

En ese sentido, se han realizado sesiones informativas para que las dependencias y entidades conozcan el contenido y alcances de un documento de seguridad de sistemas de datos personales (el cual es obligatorio), a efecto de aclarar dudas concretas y acompañar a los servidores públicos responsables del tratamiento de datos y de áreas de tecnologías de la información, en la tarea de identificar sus riesgos para que, a partir de ellos, cada uno elaborare una política de gestión de la seguridad ad-hoc. El énfasis se ha puesto por tanto, en garantizar la integridad, confidencialidad y disponibilidad de la información personal, así como contar con planes para enfrentar contingencias concretas.

Finalmente, cuando los sistemas involucran el tratamiento de datos biométricos, cabe hacer mención, que el Instituto considera y ha citado, a manera de referencia, el documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003, por el Grupo del artículo 29,11 con relación al uso de huellas dactilares. Del mismo modo, se ha hecho mención al estudio Fingerprint Vendor Technology Evaluation, publicado por el National Institute of Standards and Technology.12

Nuevos retos a enfrentar

La actuación del IFAI como órgano garante en materia de protección de datos personales, comienza a implantarse cotidianamente en el quehacer de las oficinas gubernamentales.

Otra de las prioridades del IFAI en el mediano plazo, es efectuar evaluaciones del impacto a la privacidad (PIA) ex ante el lanzamiento de grandes proyectos que involucran la utilización de nuevas tecnologías e información de las personas.

En ese rubro, se contrató a través de una licitación pública internacional los servicios de un consultor especializado para llevar a cabo una PIA para un Anteproyecto de Norma Oficial Mexicana, que implementará un expediente clínico electrónico bajo un formato estándar para todos los mexicanos. A p

artir de los hallazgos del consultor, el IFAI emitió recomendaciones específicas a la Secretaría de Salud para su observancia, de modo que la información personal contenida en historias clínicas electrónicas, esté debidamente protegida.

Otra asignatura pendiente es efectuar, a su vez, un análisis de mitigación de los impactos a la privacidad del proyecto para la emisión de una cédula de identidad ciudadana. Sobre este proyecto me complacerá compartir nuestra experiencia en futuras publicaciones.

Notas

1 Peschard Mariscal, Jacqueline, "The Federal Institute of Access to Public Information as the Guarantor Entity for the Protection of Personal Data", dataprotectionreview.eu, número 10, Madrid, España, octubre, 2009. Versión en español.

2 El Instituto Federal de Acceso a la Información Pública es un organismo descentralizado, no sectorizado, con autonomía operativa, presupuestaria y de decisión, en términos de lo establecido en el su Decreto de Creación , publicado en el Diario Oficial de la Federación el 24 de diciembre de 2002.

3 Ley Federal de Transparencia y Acceso a la Información Pública , publicada en el Diario Oficial de la Federación, el 11 de junio de 2002 y reformada mediante Decreto publicado en el citado órgano informativo el 6 de junio de 2006.

4 De junio de 2003 a septiembre de 2009, se cuenta con los siguientes datos:

- Total de solicitudes de acceso a la información presentadas: 456,335
- Total de recursos (quejas) ante el IFAI: 23,531

Para consultar mayores detalles ver:http://www.ifai.org.mx/descargar.php?r=/pdf/gobierno/&a=stats.pdf.

5 Lineamientos de protección de datos personales , publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.

6 Con la reforma al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 1 de junio de 2009, se reconoce el derecho de toda persona a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición; no obstante, no se cuenta todavía con una ley reglamentaria que permita el ejercicio de los derechos de cancelación y oposición a nivel Federal, por lo que hasta en tanto no se legisle en consecuencia, el ejercicio de los derechos de protección de datos personales se encuentra limitando al de acceso y corrección (rectificación), en los términos que establece la Ley de Trasparencia. Respecto a las leyes reglamentarias, no se omite señalar que algunos estados de la República Mexicana, como Colima y el propio Distrito Federal ya cuentan con leyes específicas en materia de protección de datos personales.

7 Artículos 55 y 56 del Reglamento Interior de la Secretaría de Gobernación. Disponible en http://www.ordenjuridico.gob.mx/Federal/Combo/R-273.pdf.

8 Disponible para consulta en http://www.diputados.gob.mx/LeyesBiblio/doc/140.doc.

9 Disponible para consulta en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGP.doc.

10 En términos del artículo 251 de la Ley del Seguro Social, el Instituto Mexicano del Seguro Social, tiene dentro de sus atribuciones y facultades, administrar los seguros de riesgos de trabajo, enfermedades y maternidad, invalidez y vida, guarderías y prestaciones sociales, salud para la familia, adicionales y otros, así como prestar los servicios de beneficio colectivo que señala su propia ley, y en general los asuntos relacionados con la asistencia social de sus derechohabientes, entre otros. Ley del Seguro Social, disponible en: http://www.diputados.gob.mx/LeyesBiblio/doc/92.doc.

11Para consulta en: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/rules-art-29_en.pdf.

12 Es un organismo federal, dentro del Departamento de Comercio de los Estados Unidos de América, cuya misión es promover la innovación y la competitividad industrial mediante la promoción de la ciencia y la tecnología en formas que mejoren la seguridad económica, entre otras funciones. Fingerprint Vendor Technology Evaluation 2003. National Institute of Standards and Technology (NIST), pp. 14 y 15.