Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Ciudad de México, a 6 de enero de 2018
INAI/006/18

ACONSEJA INAI EXTREMAR PRECAUCIONES AL PROPORCIONAR INFORMACIÓN PARA IDENTIFICACIÓN BIOMÉTRICA

- **El Instituto advirtió la existencia de un creciente uso de sistemas de identificación biométrica, por lo que recomendó ser cuidadoso con su utilización y así evitar la comisión de delitos como el robo de identidad**

Ante el incremento en el uso de sistemas de identificación biométricos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) recomienda ser cuidadoso con su utilización, para prevenir delitos como el robo de identidad.

Un sistema de autenticación biométrico recurre a técnicas como la lectura de huellas dactilares, el reconocimiento de iris, el análisis de retina, el reconocimiento facial y de voz, entre otros.

Actualmente diversas instituciones están incorporando sistemas de autenticación biométrica con el objetivo de generar alternativas que garanticen mayor seguridad a sus sistemas de información.

Este tipo de sistemas hacen uso de datos personales, lo que conlleva una alta responsabilidad para los responsables de tratar esta información, subraya el organismo garante.

Añadió que los datos personales biométricos no pueden cambiarse, como una contraseña alfanumérica, por ejemplo, que puede renovarse con cierta periodicidad e incluso eliminarse cuando ya nos sea necesaria, mientras que la información biométrica es inherente a la persona y no hay posibilidad de modificarla.

Cabe recordar que durante el Congreso *Chaos Computers Club*, en Alemania, se reveló que un *hacker* dijo haber reproducido la huella dactilar de la Ministro de Defensa alemana Ursula Von Der Leyen, a partir de una serie de fotografías publicadas en medios de comunicación oficiales.

El *hacker* señaló que eso fue posible gracias a la utilización de un software comercial llamado *VeriFinger*, lo que puso en evidencia la facilidad con la que un dato biométrico podría ser replicado indebidamente ante el más mínimo descuido.

En este contexto, el INAI emitió las siguientes recomendaciones para los titulares de los datos personales en la utilización de la autenticación biométrica en la banca móvil:

Primero. Informarse sobre los riesgos relacionados con el tratamiento de datos biométricos para tomar decisiones más informadas respecto del uso de éstos.

Segundo. Estar al tanto de la política y/o aviso de privacidad de las aplicaciones de banca móvil con el objeto de informarse sobre:

a) Los datos personales biométricos que serán recabados. De preferencia, se recomienda que los responsables no conserven los datos biométricos, sino que reciba sólo los datos digitalizados con el fin de autenticar la identidad del usuario.
b) Las finalidades y uso que se dará a dichos datos.
c) Las medidas de seguridad que implementará el responsable para proteger los datos personales biométricos.
d) Los derechos que tiene en relación con el tratamiento de sus datos biométricos.

Tercero. Descargar aplicaciones de banca móvil únicamente en los mercados de aplicaciones autorizados.

Cuarto. La utilización de servicios de identificación biométrica, en general, es opcional, por lo que es decisión de cada titular de los datos personales permitir ese esquema de identificación. Por ello se recomienda autorizar su uso sólo en caso de considerarlo necesario y siempre que se esté seguro de que existen suficientes medidas de seguridad para protegerlos.

Quinto. Proporcionar el menor número de datos biométricos que sea posible.

Sexto. Utilizar el servicio de autenticación biométrica como método secundario de protección que complemente los otros métodos de seguridad, pero sin reemplazarlos del todo.

El INAI recordó que la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) establece que los responsables de los sistemas de información personal deberán informar, de forma inmediata, a los titulares de los datos sobre aquellas vulneraciones de seguridad que afecten de forma significativa sus derechos patrimoniales.

Para conocer más sobre estos derechos consultar www.inai.org.mx.

-o0o-