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

Ciudad de México, a 30 de julio de 2017
INAI/239/17

INAI PRESENTA RECOMENDACIONES PARA USUARIOS DE SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA EN LA BANCA MÓVIL

- **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**

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) advirtió la existencia de un creciente uso de sistemas de identificación biométricos, por lo que recomienda ser cuidadoso con su utilización y así evitar la comisión de delitos como el robo de identidad.

El Instituto indicó que la autenticación biométrica consiste en la identificación de una persona específica a través de la obtención y utilización de datos biométricos. Un sistema de autenticación biométrico puede incluir técnicas como la lectura de huellas dactilares, el reconocimiento de iris, el análisis de retina, el reconocimiento facial y de voz, entre otros.

Señaló que diversas instituciones del ámbito financiero, particularmente, se han dado a la tarea de buscar alternativas que garanticen mayor seguridad informática a sus sistemas de información y a sus cuentahabientes, en el manejo de los servicios electrónicos que ofrecen.

Sin embargo, expuso el órgano garante de la protección de los datos personales, el uso de sistemas de autenticación biométricos, derivado de su progresiva utilización y, sobre todo, del tipo de servicios y datos personales a los que permite el acceso, conlleva una alta responsabilidad para sus titulares; por lo tanto se recomienda que las personas sean particularmente cuidadosas con los mismos y eviten compartirlos o comunicarlos indiscriminadamente.

El INAI hizo notar que en el caso de los datos personales biométricos el riesgo es mayor ya que no pueden cambiarse, toda vez que, si a un usuario le es robada una contraseña, éste puede generar una nueva; sin embargo, tratándose de huellas dactilares, por ejemplo, no existe tal alternativa.

Recordó 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-