LEYES DE PROTECCIÓN DE DATOS PERSONALES EN EL MUNDO Y LA PROTECCIÓN DE DATOS BIOMÉTRICOS PARTE 2

Isai Rojas González
Gabriel Sánchez Pérez

biometría

numero-14

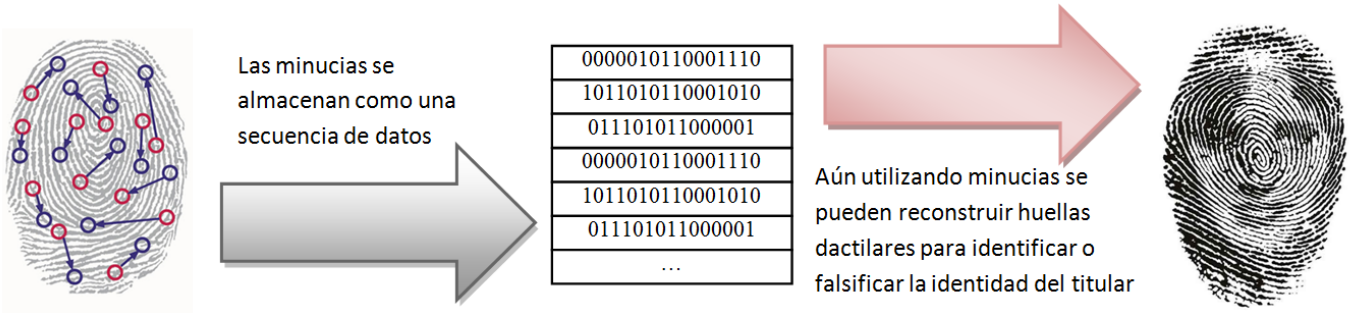
En la primera entrega del artículo se describieron conceptos básicos referentes a la protección de datos personales y a la biometría, se hizo una breve introducción a las leyes y acuerdos de protección de datos personales que existen en el mundo y se enumeraron algunos de los casos más relevantes con el objetivo de dar a conocer los antecedentes que existen respecto a cómo son considerados los datos biométricos por las leyes de protección de datos personales de distintos países en el mundo.

En esta segunda parte se describen algunos de los riesgos que están asociados al uso de datos biométricos y que motivan a la búsqueda de medidas de protección, se habla de la forma en que éstos son considerados a nivel internacional, sobre el contexto de las leyes de protección de datos personales y sobre una serie de recomendaciones emitidas por organismos internacionales referentes a cómo deben ser obtenida y procesada esta información.

RIESGOS ASOCIADOS AL USO DE DATOS BIOMÉTRICOS

Un sistema biométrico que no es protegido adecuadamente puede facilitar la obtención de información personal sensible. Por ejemplo, si un atacante roba la base de datos de un sistema de reconocimiento facial en el cual se almacenan fotografías, se podría inferir la raza de cada uno de los usuarios, lo que podría ser causa de discriminación u otras acciones.

Algunos datos biométricos pueden ser obtenidos realizando el proceso inverso de captura y almacenamiento, como es el caso de las huellas dactilares. Éstas tienen rasgos únicos conocidos como minucias, durante el proceso de captura, estos son identificados y codificados para después almacenarlos como una secuencia de datos denominada plantilla de minucias, de tal forma que, en lugar de almacenar una fotografía de la huella dactilar, se almacenan plantillas de minucias. Se dice que *una huella dactilar reconstruida a partir de la plantilla de minucias* ***[1]*** *tiene un resultado positivo en más del 90% de los casos, y que este tipo de reconstrucciones son más frecuentes de lo que se podría suponer*[2]. Esto indica que pueden identificarse personas o falsificar identidades mediante huellas dactilares que son obtenidas exitosamente, en su forma original, incluso desde una base de datos de plantillas de minucias.



En 2003, el Grupo de Protección de las Personas en lo que Respecta al Tratamiento de Datos Personales, creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, adoptó un documento de trabajo sobre biometría, en la introducción del documento se puede apreciar la siguiente inquietud:

…Una utilización amplia y sin control de la biometría es preocupante desde el punto de vista de la protección de los derechos y libertades fundamentales de las personas. Este tipo de datos es de una naturaleza especial, ya que tienen que ver con las características comportamentales y fisiológicas de una persona y pueden permitir su identificación inequívoca… **[3]**

La recolección de datos biométricos es otro aspecto de preocupación, así lo señala la Comisión Nacional de Informática y Libertades (Francia) [4] en su informe de actividades del año 2007, que en uno de sus fragmentos dice: … *Algunos datos biométricos* presentan la particularidad de poder ser recabados y utilizados sin que el interesado se dé cuenta. Es el caso de las huellas genéticas, ya que todos vamos dejando involuntariamente un rastro de nuestro

cuerpo, aunque sea ínfimo, del cual se puede extraer el código ADN. Lo mismo sucede con las huellas dactilares, de las que también vamos dejando un rastro, más o menos fácil de procesar, en nuestra vida cotidiana[5]. La Comisión indica que la biometría con rastro requiere de medidas de seguridad especiales para garantizar la protección de las personas afectadas.

PROTECCIÓN JURÍDICA DE LOS DATOS BIOMÉTRICOS

Por su naturaleza, los datos biométricos son datos personales, sin embargo, en muy pocas legislaciones en el mundo se consideran de manera explícita como datos personales y menos aún como datos personales sensibles, lo anterior da origen a diversas controversias.

En España y Argentina, las leyes de protección de datos personales, no han tipificado de manera explícita a los datos biométricos, es por ello que organismos regulatorios han sido los encargados de debatir y emitir resoluciones para cada caso específico de controversia, lo han hecho evaluando las circunstancias particulares de cada situación.

En el año 2006, la Agencia Española de Protección de Datos resuelve que el uso de la huella dactilar como medio para controlar el acceso de alumnos al colegio resulta excesivo y desproporcionado para esa finalidad.

Por otro lado, en Argentina en el 2009, la Dirección Nacional de Protección de Datos Personales resolvió, respecto a un banco de datos de aficionados al fútbol, que pueden ser tratados los datos biométricos, por ser datos estrictamente de identificación, cuando sean necesarios para la finalidad pretendida (seguridad en estadios de fútbol).

La mayoría de las leyes de protección de datos personales en el mundo se encuentran en una situación de ambigüedad en lo que se refiere a los datos biométricos. La legislación en México tiene el mismo inconveniente, la ley en sí no hace mención explícita de los datos biométricos ni de su tratamiento.

Algunos países comienzan a incluir de manera explícita el concepto de datos biométricos y la manera en que estos deben tratarse y protegerse:

Australia. El comité de reforma de la ley de privacidad, recomendó que se agregaran los datos biométricos a la definición de datos sensibles. El cambio aún no ha sido incluido en la versión actual de la ley con fecha del 4 de julio de 2011.

Rusia. Actualmente, se encuentra en proceso de modificación a su ley federal de protección de datos de 2006, el propósito es mejorar algunos aspectos de seguridad. Uno de los cambios indica que el reglamento establecerá los requisitos de seguridad para el procesamiento de datos biométricos.

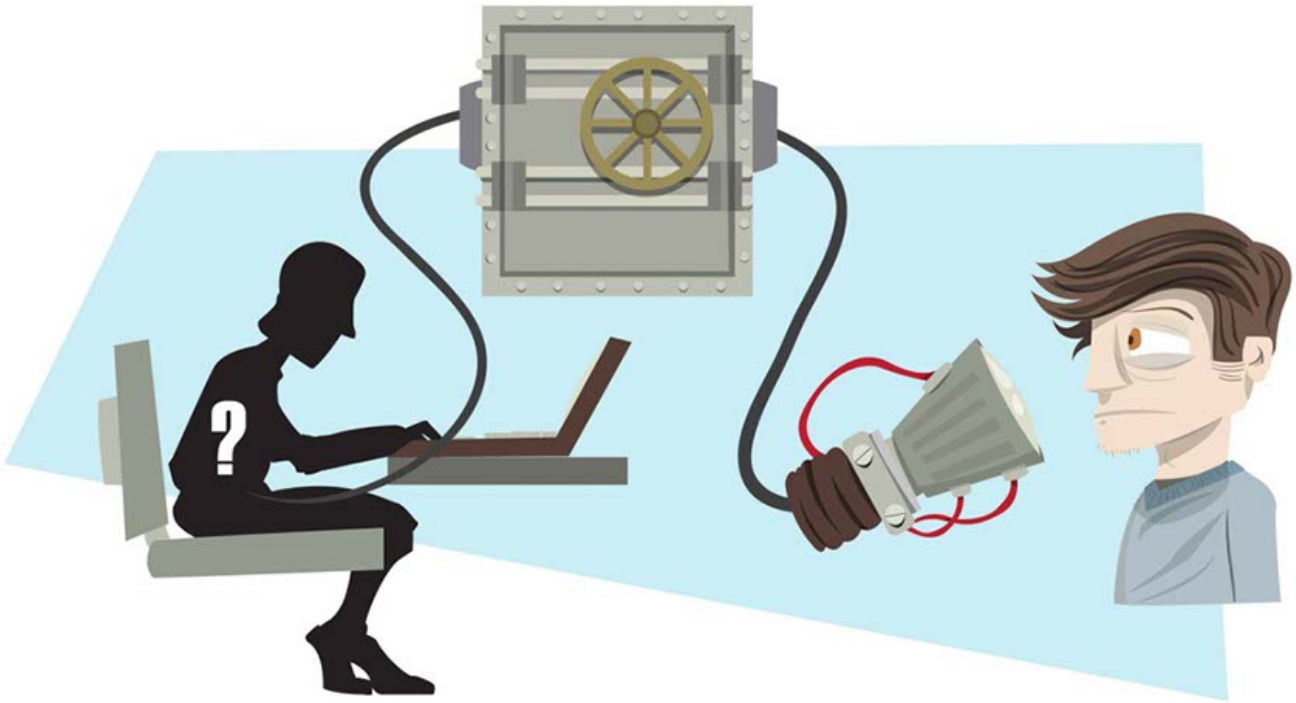
Perú. Recientemente adoptó la ley número 29.733 que se refiere a la protección de datos personales y señala en su artículo 2º que los datos biométricos son datos personales sensibles.

Futura legislación en Colombia. El documento con el texto conciliado y aprobado del proyecto de ley estatutaria número 184 de 2010 Senado, 046 de 2010 Cámara en Colombia, especifica en su título III, artículo 5º que los datos biométricos son considerados datos personales sensibles.

Convenios internacionales. El Consejo de Europa (Council of Europe)[6] ha publicado un documento llamado: “Informe de situación relativo a la aplicación de los principios de la convención 108 sobre la recogida y al proceso de los datos biométricos”[7], el informe contiene una serie de pronunciamientos respecto a los datos biométricos y su uso. A continuación, se presenta la idea básica de cada punto:

1. Los datos biométricos deben ser considerados como una categoría específica de datos, ya que estos siguen siendo los mismos en distintos sistemas y son inalterables de por vida.

2. Antes de recurrir a la biometría, se deben evaluar: las finalidades previstas para los datos, las ventajas contra los inconvenientes que afecten la vida privada de la persona involucrada, y se deben tener posibles soluciones alternativas que supongan un menor atentado contra la privacidad.
3. No se debería optar por la biometría únicamente por el hecho de que su uso resulte práctico.
4. Los datos biométricos deben ser utilizados con fines determinados, explícitos y legítimos. No deben ser procesados de manera incompatible con esas finalidades.
5. Los datos deberían ser adecuados, pertinentes y no excesivos en comparación con la finalidad del proceso; si basta con patrones, se debería evitar el almacenamiento de la imagen biométrica.
6. A la hora de elegir la estructura del sistema, se debería proceder teniendo en mente los aspectos de seguridad.
7. La estructura de un sistema biométrico no debería ser desproporcionada respecto a la finalidad del proceso; si basta con la verificación, no se debería desarrollar una solución de identificación.
8. La persona afectada debería ser informada de la finalidad del sistema y de la identidad del responsable del proceso. Además, conocer los datos procesados y las categorías de personas a las que se comunicarán esos datos.
9. La persona afectada tiene derecho de acceso, rectificación, bloqueo y cancelación de sus datos.
10. Se deben prever medidas, técnicas y organizativas, que sean adecuadas para proteger los datos biométricos contra la destrucción y la pérdida accidental, también se deben proteger contra el acceso, modificación o comunicación no autorizada y deben ser resguardados de cualquier otra forma de procesamiento ilícito.
11. Se debería desarrollar un procedimiento de certificación y de control, con el fin de establecer normas de calidad para el software y la formación del personal responsable del registro y la verificación de datos biométricos. Se recomienda una auditoría periódica que pruebe las cualidades técnicas del sistema.
12. Si una persona, registrada en un sistema biométrico, es rechazada, el responsable de proceso debería, a petición de ésta, volver a examinar el caso y si fuese preciso, ofrecerle soluciones de sustitución adecuadas.



Actualmente, hay varios países que cuentan con leyes de protección de datos personales, pero pocos son los que incluyen en sus postulados, de manera explícita, a los datos biométricos y el tratamiento que éstos deben tener, el precedente legal lo establecen países como Rusia, Perú y Colombia.

Es necesario regular al respecto del uso de los datos biométricos en los sistemas de información, son datos muy íntimos que acompañan a su titular de por vida y que no pueden ser cancelados o restablecidos; si a un usuario le roban y falsifican su huella dactilar, esta no podrá ser cancelada, su huella seguirá siendo la misma.

La regulación legal de los datos biométricos ayuda a prevenir ambigüedades que pueden generar controversias y además establece las reglas necesarias para el correcto resguardo de la información sensible de las personas.

Referencias

[1] Remolina A. N. (2011). Sistemas de identificación biométrica y protección de datos personales: ni “tecnofobia”, ni “tecnofascinación”, pero sí “tecnoreflexión”. Consultado en:

http://www.ambitojuridico.com/BancoConocimiento/N/noti-111116-06_(sistemas_de_identificacion_biometrica_y_proteccion_de_datos_personales)/noti-111116-06_(sistemas_de_identificacion_biometrica_y_proteccion_de_datos_personales).asp

[2] Comité consultivo de la Convención para la protección de las personas respecto al proceso

automatizado de los datos de carácter personal (T-PD) (2005). Informe de situación relativo a la aplicación de los principios de la convención 108 a la recogida y al proceso de los datos biométricos

[3] Sitio Web Kimaldi Electrónics. Tratamiento de la huella digital de los trabajadores/as.

[4] Agencia Española de Protección de Datos:

- Proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. Informe 368/2006
- Tratamiento de la huella digital de los trabajadores.
- Resolución de archivo de actuaciones. Expediente Nº: E/00016/2007

[5] Segalis B. (2011). Russia Amends Federal Data Protection Law; Privacy Enforcement on the Rise. Consultada en: http://www.infolawgroup.com/2011/07/articles/international-2/russia-amen...

[6] Kindt E. (2007). Biometric applications and the data protection legislation. Datenschutz und Datensicherheit.

[7] Woo R. B. Challenges posed by biometric technology on data privacy protection and the way forward

[8] Liu Y. (2007). Introduction to biometrics from a legal perspective. University of Oslo.

[8] Liu Y. (2008). Identifying Legal Concerns in the Biometric Context. Journal of International Commercial Law and Technology Vol. 3, Issue 1. University of Oslo.

[9] Iglezakis I. (2010). EU data protection legislation and case-law with regard to biometric applications. Faculty of Law, Aristotle University of Thessaloniki.

[10] El Congreso de Colombia. Texto conciliado y aprobado del proyecto de Ley Estatutaria número 184 de 2010 Senado, 046 de 2010 Cámara. “Por la cual se dictan disposiciones generales para la protección de datos personales”.

[11] Cavoukian A. (2008). Fingerprint Biometrics: Address Privacy Before Deployment

[12] Article 29 of Directive 95/46/EC – Data Protection Working Party. Working document on biometrics (2003)

[13] Australia. Privacy Act 1988. Act No. 119 of 1988 as amended. This compilation was prepared on 4 July 2011 taking into account amendments up to Act No. 60 of 2011.

Enlaces Web:

[1] http://cyberlaw.stanford.edu/profile/david-banisar

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:e...

[3] http://www.statewatch.org/news/2004/feb/biometric-wp80_en.pdf

[4] http://www.martinaberastegue.com/seguridad/privacidad/legislacion-intern...

[5] http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/commo...

Coautores de este artículo:

Linda Karina Toscano Medina, María del Carmen Prudente Tíxteco y Gualberto Aguilar Torres

---

[1] Plantilla de minucias: Se denomina al conjunto de características ínfimas de una huella dactilar que se almacenan como un patrón de datos único que hace identificable de manera inequívoca al titular de la huella.

[2] *Fingerprint Biometrics: Address Privacy Before Deployment*. Publicado por el Comisionado de Información y Privacidad de Ontario en noviembre de 2008.

[3] http://www.informatica-juridica.com/anexos/anexo545.asp

[4] http://www.cnil.fr/

[5] http://www.cnil.fr/fileadmin/documents/es/CNIL-rapport2007-VE.pdf

[6] Sitio Web: http://www.coe.int

[7] Se puede consultar la versión completa en: http://www.coe.int/t/dlapil/codexter/Source/Working_Documents/2005/T-PD _2005_ BIOM F.pdf

---