

Sistemas biométricos en materia criminal: un estudio comparado*

Biometric criminal databases: a comparative study

Vanessa Díaz Rodríguez**

RESUMEN

Hay un interés creciente en la implementación de sistemas biométricos encaminados a la identificación. La biometría no es una práctica nueva; y ha estado en uso desde 1858. El reconocimiento facial, dactilar y del iris son los sistemas biométricos más comunes. Este artículo aborda los sistemas biométricos según la ley, y plantea además un estudio comparativo en Australia, México, Nueva Zelanda y España, cuyos sistemas nacionales en materia criminal no operan del mismo modo. El artículo destaca las bases de datos de la Interpol, ya que reflejan las mejores prácticas en materia criminal. Esta investigación concluye que los sistemas biométricos, en particular aquellos en materia criminal, suponen retos específicos para la privacidad y los derechos de protección de datos, no sólo a nivel nacional sino también a nivel internacional.

PALABRAS CLAVE: Datos biométricos, sistemas biométricos, bases de datos biométricos en materia criminal, perfiles biométricos en materia criminal.

ABSTRACT

There is an increasing interest in the implementation of biometric systems for identification purposes. Biometrics is not new; and has been in use since 1858. Facial, fingerprints and iris recognition are the most common biometric systems in use. This paper is about biometric systems deployment in law enforcement. The research involves a comparative study in Australia, Mexico, New Zealand and Spain where national biometric criminal databases are operating with asymmetries among them. The paper highlights Interpol's databases because it represents the best practices of the extent of biometric criminal databases. It concludes that biometric systems pose singular challenges to privacy and data protection rights, particularly biometric criminal databases, not only at national level also at international level.

KEY WORDS: Biometric data, biometric systems, biometric criminal databases, criminal biometric profiles.

* Recibido: 12 de julio de 2012. Aceptado: 20 de agosto de 2012.

** Doctorante en Derecho por la Facultad de Derecho de la Universidad de Tasmania, Australia.
(vanediazrod@yahoo.com).

Sumario

1. Introducción
2. Algunos referentes históricos de sistemas biométricos
3. Sistemas biométricos: funciones y objetivos
4. Bases biométricas en materia criminal
 - A) Bases de datos biométricas internacionales
 - B) Bases biométricas en materia criminal en Australia, México, Nueva Zelanda y España
5. Conclusiones

1. Introducción

La biometría no es algo nuevo. La historia revela que la diversidad humana y la estructura de la población han sido estudiadas utilizando la biometría. Actualmente existe un debate doctrinal referente a la acepción del término “biometría”. Para algunos doctrinarios es una técnica, pero para otros es una ciencia.¹ Los términos “biometría” y “biométricos” provienen del latín *bios*, vida, y *metría*, medidas. Por tanto, los datos biométricos constituyen información referente a las medidas y características tanto fisiológicas como morfológicas de los seres vivos a través de técnicas manuales o automatizadas.

Esta investigación identifica de manera breve los referentes históricos más importantes de la biometría. En este sentido, se reconoce que tanto la eugenesia como la genética comparten los mismos antecedentes históricos de la biometría. Siendo las huellas dactilares los primeros datos biométricos obtenidos a través de sistemas manuales que con el tiempo se han ido perfeccionando.

Los sistemas biométricos solamente tienen dos objetivos. El primero es para identificar, es decir, reconocer al individuo, por lo que su funcionamiento está basado en utilizar un dato y compararlo con una lista o base de datos (comparación 1:N). El segundo es para autenticar, es decir, verificar la identidad del

¹ Al analizar la literatura especializada de la materia, vemos que se puede clasificar en dos grupos. En el primer grupo se ubican aquellas obras que consideran a la biometría como “técnica” que a través de la estadística auxilia a diferentes ciencias para resolver problemas. *Cfr.* KING, ROBERT C. y WILLIAM D. STANSFIELD, *A Dictionary of Genetics*, 5a. ed., Oxford University Press, Nueva York, 1997; *cfr.* SOKAL, ROBERT y ROHLF, JAMES. *Biometry*, 3a. ed., W. H. Freeman and Company, Estados Unidos, 2003; *cfr.* SOKAL, ROBERT y ROHLF, JAMES. *Introduction to Biostatistics*, W. H. Freeman and Company, Estados Unidos, 1973; *cfr.* ZHANG, DAVID D. *Automated Biometrics Technologies and Systems*, Kluwer Academic Publishers, Estados Unidos, 2000.

Mientras que en el segundo grupo encontramos autores que consideran a la biometría como “ciencia”. *Cfr.* HOPKINS, RICHARD. “An introduction to biometrics and large scale civilian identification”, en *International Review of Law, Computers & Technology*, No. 13, pp. 337-363; *cfr.* MATHER, KENNETH y JINKS, JOHN L. *Biometrical Genetics. The Study of Continuous Variation*, Cornell University Press, Estados Unidos, 1971.

VANESSA DÍAZ RODRÍGUEZ

individuo, por lo que su funcionamiento está basado en la utilización de un dato comparándolo con el mismo dato almacenado previamente (comparación 1:1).

Por tanto, nuestra investigación se centra en las bases biométricas en materia criminal como un caso de estudio. Las bases de datos biométricas en materia criminal se han incrementado tanto a nivel nacional como a nivel internacional por cuestiones de cooperación internacional policiaca y judicial. La investigación resalta como caso de buena práctica o de éxito las bases de datos de Interpol. En este mismo sentido, se realiza un estudio comparado a nivel nacional entre Australia, México, Nueva Zelanda y España.

La investigación revela cuatro cuestiones fundamentales que deben tomarse en cuenta en la implementación de cualquier tipo de bases de datos, pero aún más tratándose de bases de datos biométricas: ¿qué personas se encuentran en esas bases de datos? ¿Cuánto tiempo debe almacenarse la información? ¿Quién tiene acceso a la información contenida en las bases de datos biométricas? Y, finalmente, la protección de la privacidad en el flujo de información.

Este artículo se encuentra dividido en cinco secciones. La primera se refiere al objeto de estudio; en la segunda se establecen los referentes históricos de los sistemas biométricos; en la tercera se abordan las principales funciones y objetivos de los sistemas biométricos; en la cuarta sección se desarrollan las bases biométricas en materia criminal. Especial referencia a nivel internacional de las bases de datos de Interpol y a nivel nacional, como estudio comparado, las principales bases de datos biométricas de Australia, México, Nueva Zelanda y España, y en la última se desarrollan las conclusiones.

2. Algunos referentes históricos de sistemas biométricos

En esta sección se establecerán de manera breve algunos referentes históricos de los sistemas biométricos. Pero antes debemos establecer el origen histórico del término biométrico. De acuerdo con la bibliografía básica, a PEARSON y WELDON se les atribuye haber acuñado el término biometría (*biometry*),² pero ya en 1841, BERNOULLI usó el término “biométrico” (*biometric*).³

El primer antecedente histórico registrado data de 1858. HERSCHEL estampó la huella de la palma de la mano de todos y cada uno de sus trabajadores al reverso

² SOKAL, ROBERT Y ROHLF, JAMES. *ibidem*, p. 3; NORTON, B. J. “The Biometric Defense of Darwinism”, en *Journal of the History of Biology*, No. 6, pp. 283-316.

³ “En 1896, Galton había jugado con la palabra ‘filometría’ y Pearson, por su parte, sugirió el término ‘biometría’ ‘para la ciencia que aplica en la teoría moderna de las estadísticas el estudio de la variación y correlación en forma viva’”. ARMITAGE, PETER. “Biometry and Medical Statistics”, en *Biometrics*, No. 41, pp. 823-833 (la traducción es nuestra).

de los contratos para poder identificar a sus trabajadores de otras personas que podrían exigir el pago de sus actividades.⁴ Al año siguiente DARWIN publicó su obra *El origen de las especies*. Debemos recordar que durante aquellos años el interés por el tema de la “evolución” fue muy relevante. En 1866, MENDEL descubrió lo que hoy llamamos *Leyes de la herencia de Mendel*, y dos años más tarde DARWIN publicó *La variación de animales y plantas domesticados*.⁵

Para 1869, WILSON había medido 464 cráneos de delincuentes; su investigación arrojó datos como la constante sobre “el tamaño medio inferior del cráneo a la de la población normal”,⁶ y llegó a la conclusión de que “la deficiencia craneal se asocia con el deterioro físico de los seres humanos”.⁷ Veinte años después de que DARWIN publicara *El origen de las especies*, la idea de la evolución seguía siendo un tema popular y ganó demasiados adeptos; como muestra de esta euforia se encuentra la publicación de *La herencia del genio* elaborada por GALTON.⁸

La mayor contribución de GALTON a la biología es “la aplicación de la metodología estadística para el análisis de la variación biológica, tal como el análisis de la variabilidad y su estudio de regresión y correlación en las mediciones biológicas”.⁹

En 1890, HERSCHEL envió sus registros a GALTON, y dos años más tarde se confirmaría que las huellas dactilares de un individuo no cambian con el simple transcurso del tiempo.¹⁰ Recordemos que en ese entonces el método de identificación utilizado era el Bertillonage, que consistía en la medición de distintas partes del cuerpo y marcas individuales —como tatuajes o cicatrices— para identificar a los criminales. Este método fue desarrollado por BERTILLON, oficial de la policía francesa, en 1883.¹¹

Cabe destacar que BERTILLON desarrolló la “fotografía métrica” en donde se estandarizan las fotografías de identificación e imágenes visuales de las escenas de los crímenes. Actualmente se encuentran vigentes las reglas de la fotografía métrica de BERTILLON en la ciencia forense.¹²

⁴ Cfr. HERSCHEL, WILLIAM J. *The Origin of Finger-Printing*, Oxford University Press, 1916. Edición digital de Gavan Tredoux en <http://galton.org/fingerprints/books/herschel/herschel-1916-origins-1up.pdf> (9 de diciembre de 2012).

⁵ Cfr. SCHWARTZ COWAN, RUTH. “Francis Galton's Statistical Ideas: The Influence of Eugenics”, en *The University of Chicago Press on behalf of The History of Science Society*, No. 4, pp. 509-528.

⁶ CLOUSTON, T. S. “The Developmental Aspects of Criminal Anthropology”, en *The Journal of the Antropological Institute of Great Britain and Ireland*, No. 23, pp. 215-225.

⁷ *Idem*.

⁸ Cfr. SCHWARTZ COWAN, RUTH. “Francis Galton's Statistical Ideas: The Influence of Eugenics”, *op. cit.*

⁹ SOKAL, ROBERT y ROHLF, JAMES. *Biometry*, *op. cit.*, p. 4.

¹⁰ Cfr. SCHWARTZ COWAN, RUTH. *op. cit.*

¹¹ “Bertillon system”, en *Encyclopædia Britannica Online*, 2012. Disponible en línea: <http://www.britannica.com/EBchecked/topic/62832/Bertillon-system> (9 de diciembre de 2012).

¹² *Idem*.

Sin embargo, en 1891, VUCETICH, un croata nacionalizado argentino, perfeccionó el sistema galtoniano; presentó un sistema de clasificación básico de huellas dactilares de la mano.¹³ Más tarde, en 1896, el sistema de clasificación de Henry permite la categorización lógica de diez registros de impresión de huellas dactilares en agrupaciones primarias basadas en tipos de patrones de dichas huellas.¹⁴ En consecuencia, las huellas dactilares son el más antiguo sistema de identificación biométrica.

Los estudios de variación biológica fueron expuestos por PEARSON y WELDON, quienes implementaron la metodología estadística en dichos estudios.¹⁵ Ahora bien, el desarrollo de la biometría comparte aspectos históricos tanto de la Genética¹⁶ como de la Eugenesia. Etimológicamente, la Eugenesia hace referencia al “buen nacimiento”. Se trata de una disciplina, promovida por GALTON, que busca mejorar los rasgos hereditarios mediante varias formas de intervención.¹⁷

Durante este periodo, la idea de que todas las debilidades humanas son el resultado de una genética “pobre” creció a tal grado que la posición social era determinada por la genética. En Europa, Lombroso y sus pupilos desarrollaron la teoría antropológica criminal.¹⁸

La Eugenesia fue institucionalizada principalmente en el norte de Europa y Estados Unidos de América. El sistema migratorio de Estados Unidos de América, por ejemplo, consideraba como perjudicial para la población “americana” la aceptación de inmigrantes provenientes de estratos económicos y sociales pobres. Sin embargo, fue en Alemania, en el periodo nazi, donde la clase y los prejuicios raciales eran frecuentes y generalizados.¹⁹

Lo novedoso de la historia de la biometría es que la mayoría de los sistemas biométricos se basan en ideas literarias, en específico de novelas, que son llevadas al cine y televisión incluso antes de ser desarrolladas y perfeccionadas; la mayoría son financiadas por el gobierno para después comercializar el producto.

¹³ LOCARD, EDMOND. *Manual de técnica policiaca*, Editorial Maxtor, Barcelona, 1935, p. 104.

¹⁴ BEAVAN, C. *Fingerprints: The Origins of Crime Detection and the Murder Case that Launched Forensic Science*, Hyperion, Nueva York, 2001.

¹⁵ Cfr. SCHWARTZ COWAN, RUTH. *op. cit.*

¹⁶ VAN DER PLOEG, IRMA. “Genetics, Biometrics and the Informatization of the Body”, en *Ann Ist Santa*, No. 43, pp. 44-50.

¹⁷ “Eugenesia es la ciencia de la mejora de la población mediante el nacimiento controlado con características hereditarias deseadas. En el razonamiento de los eugenistas, los grupos de menores ingresos no eran pobres por falta de educación y oportunidades económicas sino porque sus capacidades morales y educativas tenían insuficiencias biológicas”. KEVLES, DANIEL J. y HOOD, LEROY (eds.). *The Code Of Codes, Scientific and Social Issues in the Human Genome Project*, Harvard University Press, Estados Unidos, 1993, p. 9.

¹⁸ Cfr. CLOUSTON, T. S. “The Developmental Aspects of Criminal Anthropology”, *The Journal of the Anthropological Institute of Great Britain and Ireland*, vol. 23, pp. 215-225.

¹⁹ Cfr. KEVLES, DANIEL J. y HOOD, LEROY (eds.). *The Code Of Codes, Scientific and Social Issues in the Human Genome Project*, *op. cit.*; cfr. BRESLER, JACK B. *Genetics and Society*, Addison-Wesley Publishing Company, Estados Unidos, 1973, p. 5.

En la siguiente tabla se muestran como ejemplos operacionales algunas de las ideas de sistemas biométricos en programas de televisión y en largometrajes utilizadas por el gobierno y la fecha en la que el producto salió a la venta.

<i>Cine y tv (ideas)</i>	<i>Sistemas biométricos automatizados</i>	<i>Utilizados por el gobierno</i>	<i>Productos comerciales</i>
The Andromeda Strain (1971)	Geometría de la mano Huella dactilar de la palma de la mano	1974 Geometría de la mano 1990 Juegos Olímpicos (Atlanta)	1980
Blade Runner (1982)	Verificación de iris	1986 usada por primera vez	1995
Tomorrow Never Dies (1997)	Reconocimiento facial	2001 Super Bowl (Florida)	--
Mission Impossible (1966-1973)	Reconocimiento de voz	1975 Primer prototipo	1980

La película *La amenaza de Andrómeda* (1971), dirigida por Robert Wise, basada en la novela homónima de Michael Crichton, mostró por primera vez el sistema biométrico relacionado con la geometría de la mano, lo cual también desencadena la posibilidad de realizar el sistema biométrico de la palma dactilar; estos sistemas fueron utilizados por primera vez en 1974 por el gobierno de Estados Unidos, pero se destaca la implementación de éstos en los Juegos Olímpicos de Atlanta, en 1990.

El segundo ejemplo que muestra la tabla es la película de *Blade Runner* (1982), dirigida por Ridley Scott y basada parcialmente en la novela de Philip K. Dick, *¿Sueñan los androides con ovejas eléctricas?* de 1968. En ésta se muestra el sistema biométrico de verificación de iris, utilizado por primera vez en 1986, cuyo producto comercial salió a la venta en 1995.

La película *El mañana nunca muere* (1997) es la décimo octava película de la serie de James Bond dirigida por Roger Spoottiswoode que muestra el sistema biométrico de reconocimiento facial. El gobierno de Estados Unidos lo implementó en 2001 durante el Super Bowl (Florida) xxxv. La policía de Tampa Bay, la Florida, utilizó el sistema biométrico de reconocimiento facial para identificar criminales.²⁰ Sin embargo, este sistema biométrico todavía no está perfecciona-

²⁰ El gobierno de los Estados Unidos de América cuenta con una de las bases de datos de reconocimiento facial más grande del mundo. Sistemas de reconocimiento facial: <http://www.faq-mac.com/noticias/sistemas-reconocimiento-facial-raul-sanchez-vitores/7477>.

VANESSA DÍAZ RODRÍGUEZ

do. Actualmente, algunos prototipos gratuitos están trabajando en redes sociales con el objetivo de perfeccionarlos para poder ser comercializados. Se destaca Facebook, Windows Live, Picasa de Google y iPhoto de Apple.

Por último, la tabla muestra la exitosa serie estadounidense de televisión *Misión Imposible* (1966 a 1973), emitida por la cadena de televisión CBS. En la cual se muestra el sistema biométrico de reconocimiento de voz, cuyo primer prototipo data de 1975, comercializado en 1980.

3. Sistemas biométricos: funciones y objetivos

El objetivo de los sistemas biométricos es la identificación (reconocimiento) o la autenticación (verificación) de los individuos sobre la base de algunas características fisiológicas o morfológicas. Se debe considerar que para el desarrollo de sistemas biométricos es fundamental distinguir precisamente su objetivo. Es decir, si el sistema biométrico va a ser utilizado para identificar o para autenticar; puesto que el reconocimiento y la verificación son actividades totalmente diferentes, y para ello algunas características fisiológicas son más apropiadas para la identificación y otras son mejor para la autenticación.²¹

Los sistemas biométricos de reconocimiento utilizan un dato y lo comparan con una lista o base de datos,²² el ejemplo más común son las bases criminales. Mientras que los sistemas biométricos de verificación sólo utilizan un dato comparándolo con el mismo dato previamente almacenado,²³ como es el caso de las bases migratorias.

Cabe señalar que no todas las características fisiológicas y morfológicas por sí mismas son datos biométricos. En algunos casos, los sistemas biométricos de reconocimiento o de autenticación podrían necesitar dos o más datos biométricos.²⁴ A lo anterior se le denomina sistemas de combinación biométrica; como ejemplos podemos señalar el tipo de sangre, el factor RH, el peso y la estatura. Considerando que el tipo de sangre por sí mismo no identifica a una persona específicamente; pero cuando se conjugan dos o más datos biométricos no hay margen de error, pues se autentifica y reconoce que esa persona, en efecto, es quien dice ser.

²¹ Cfr. BOULGOURIS, NIKOLAOS V. et al. *Biometrics, Theory, Methods, and Applications*, IEEE and WILEY, Estados Unidos, 2010; BOLLE, RUUD M. et al. *Guide to Biometrics*, Estados Unidos, 2003; cfr. ZHANG, DAVID D. *Automated Biometrics Technologies and Systems*, op. cit.

²² *Idem*.

²³ *Idem*.

²⁴ *Idem*.

Los sistemas biométricos se caracterizan por ser versátiles; es decir, estos sistemas pueden ser utilizados en diferentes áreas. Actualmente es posible encontrar sistemas biométricos en sectores tales como de salud, en servicios bancarios, en inmigración, en transporte, en telefonía, entre otros.

La implementación de sistemas biométricos también se caracteriza por la creación de bases de datos. Hoy en día la proliferación de bases biométricas se clasifican en: bases de datos de ADN (ácido desoxirribonucleico) —utilizada para desaparecidos, recién nacidos, filiación, entre otros—; bases de datos criminales —Interpol, la Plataforma México cuenta con varias bases de datos—; bases de datos migratorias —como el Sistema Integral de Operación Migratoria de México, Visas de Negocios APEC, SmartGates o puertas inteligentes de Australia y Nueva Zelanda, Eurodac, Schengen—; bases de datos poblacionales —credenciales de identidad: de Colombia, España, Alemania, Polonia, México, Argentina, entre otros—; bases de datos clínicas; base de datos electorales (como la recién anunciada credencial del Instituto Federal Electoral de México); bases de datos de licencias vehiculares o de armas, entre otras.

Con base lo anterior, se desprende que dependiendo del diseño de los sistemas biométricos, éstos pueden o no revelar mucha o poca información personal. La clasificación de datos biométricos como “sensibles” estará determinada por las circunstancias específicas. Por tanto, compartir datos biométricos con el objetivo de identificar y/o verificar a los individuos es información personal sensible.

4. Bases biométricas en material criminal

En esta sección se identifican algunos ejemplos de bases biométricas en materia criminal. Cabe señalar que la implementación de este tipo de bases de datos se ha incrementado en las últimas décadas sobre todo a nivel internacional, pero a nivel nacional el ritmo de implementación varía en cada país.

A) *Bases de datos biométricas internacionales*

35

Hoy en día hay muchos organismos y organizaciones internacionales con objetivos diferentes, pero relacionados con roles de identificación de individuos para combatir el terrorismo, crimen transfronterizo e indocumentados. Los casos más emblemáticos son las bases de datos creadas por Europol e Interpol.

En este mismo sentido, existen sistemas internacionales con objetivos similares pero con diferentes estructuras que gestionan información criminal para

VANESSA DÍAZ RODRÍGUEZ

propósitos que incluyen migración, tal como EURODAC,²⁵ el Sistema de Información Schengen II.²⁶

Esta investigación se centra en las bases de datos biométricas desarrolladas por Interpol, por considerarlas como ejemplos emblemáticos de mejores prácticas. Además, Interpol se desempeña como la única organización policial con cobertura global.²⁷ Otra razón principal para elegir la Interpol y no Europol es por la postura fijada por la Comisión de la Unión Europea de la Cámara de los Lores en su noveno informe de sesiones (2006-2007) respecto a Europol:

Europol sólo recientemente ha establecido su propio sistema de información, después de grandes retrasos. Ninguna agencia tiene suficientes conocimientos especializados pertinentes en la gestión de grandes sistemas de información. En el caso de Europol podría haber un conflicto de intereses, o al menos una percepción de uno, entre su papel como un usuario del servicio y como un proveedor de servicios, en particular, ya que se supone que sólo tienen acceso a categorías limitadas de datos.²⁸

Interpol no cuenta con equipos de policías o detectives con jurisdicciones supranacionales, tampoco van viajando alrededor del mundo para realizar investigaciones en diferentes países. Al contrario, en cada país miembro se establece una oficina nacional de Interpol denominada Oficina Central Nacional (OCN) que sirve de punto de contacto con la policía nacional o servicios de investigación.²⁹ Por su parte, los funcionarios de Interpol están obligados por las leyes nacionales de cada uno de los países miembros, pero el intercambio y flujo de información de sus bases de datos se rige por las estructuras, controles y procedimientos

²⁵ Sistema europeo de comunicaciones electrónicas entre los países de la Unión Europea (UE) y la base de datos utilizada para la comparación de las impresiones dactilares de los solicitantes de asilo y algunas otras categorías de inmigrantes ilegales. Mediante la comparación de las huellas dactilares, los países de la UE pueden determinar si un solicitante de asilo o refugiado ha solicitado previamente asilo en otro país de la UE, o bien si un solicitante entró en el territorio de la UE de manera ilegal. Reglamento (CE) No. 407/2002 del Consejo, del 28 de febrero de 2002, por el que se establecen determinadas normas de desarrollo del Reglamento (CE) No. 2725/2000 relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, *Diario Oficial* No. L 062 del 5 de marzo de 2002, pp. 0001-0005. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002R0407:ES:HTML> (30 de noviembre de 2012).

²⁶ The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *Diario Oficial*, No. L 239 del 22 de septiembre de 2000 pp. 0019-0062 [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922\(02\):EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML) (30 de septiembre de 2012).

²⁷ Interpol cuenta con 190 países miembros.

²⁸ European Union Committee of the House of Lords, *Schengen information System II (SIS II) Report with Evidence*, 9th report of session 2006/2007, marzo de 2007, Authority of the House of Lords, p. 28. <http://www.publications.parliament.uk/pa/ld200607/ldselect/lddeucom/49/49.pdf> (30 de marzo de 2012). La traducción es nuestra.

²⁹ Estructura y gobernanza de Interpol disponible en <http://www.interpol.int/es/Acerca-de-INTERPOL/Estructura-y-gobernanza/Oficinas-Centrales-Nacionales> (30 de marzo de 2012).

desarrollados por la misma Interpol, quien desarrolló una plataforma electrónica denominada i-24/7 Sistema Mundial de Comunicación Policial. El sistema interconecta todas las Oficinas Centrales Nacionales con el Cuartel General de la Interpol; permite el intercambio de información tanto policial como de investigación criminal a nivel mundial. Una de las principales ventajas de este sistema i-24/7 es precisamente el intercambio de información inmediato y directo con las autoridades policiales de cada uno de los países miembros.³⁰

Todas las bases de datos, a excepción de la base de datos de imágenes de abuso sexual infantil, son accesibles a través de la i-24/7. Las principales bases de datos disponibles en la actualidad son las siguientes:³¹

- 1) Los datos nominales.
- 2) Avisos o alertas.
- 3) Documentos de viaje robados y extraviados.
- 4) Vehículos robados.
- 5) Obras de arte robadas.
- 6) Perfiles de ADN.
- 7) Huellas dactilares.
- 8) Robo y falsificación de documentos administrativos.
- 9) Identificación de víctimas por desastres.³²
- 10) Terroristas (*fusion task force*).
- 11) Armas de fuego.

Ahora bien, con base en el Reglamento sobre el tratamiento y el intercambio de información de Interpol, los países miembros pueden intercambiar no sólo datos nominales, sino también ADN, huellas dactilares y palmares. En 2009, Interpol lanzó “i-link”, el sistema operativo desarrollado por primera vez para mejorar el intercambio de información entre los países miembros, permitiendo la interoperabilidad de sistemas o programas.

La base de datos de ADN internacional y el Sistema Automatizado de Identificación de Huellas Dactilares (AFIS por su acrónimo en inglés), utilizadas por Interpol, son bases de datos centralizadas, mientras que la base de datos Identificación de Víctimas por Desastres (Fastid) de Interpol es descentralizada. Pero, a través del “i-link” estas bases de datos son compatibles con el *software* del

³⁰ Intercambio de datos disponible en <http://www.interpol.int/es/Especialidades/Intercambio-de-datos> (30 de marzo de 2012). La traducción es nuestra.

³¹ Bases de datos <http://www.interpol.int/en/Internet/INTERPOL-expertise/Databases> (30 de noviembre de 2012). La traducción es nuestra.

³² Nueva base de datos Fastid <http://www.interpol.int/en/INTERPOL-expertise/Databases/FASTID/FAST-and-efficient-international-disaster-victim-IDentification> (30 de noviembre de 2012). La traducción es nuestra.

VANESSA DÍAZ RODRÍGUEZ

Sistema de Índice Combinado de ADN (CODIS por su acrónimo en inglés) de la Oficina Federal de Investigaciones (FBI por su acrónimo en inglés) de los Estados Unidos de Norteamérica, con el Sistema de Información de Schengen (SIS II) con la autorización del Tratado de Prüm y con la Plataforma México.

En cuanto a la base de datos de Documentos de Viaje Robados y Extraviados (SLTD por su acrónimo en inglés) cuenta con información de 145 países; algunos de estos documentos son biométricos, por ejemplo, las visas de negocios emitidas por Asia Pacífico de Cooperación Económica (APEC por su acrónimo en inglés), las visas de la zona Schengen, los pasaportes de los funcionarios de Interpol, pasaportes de Australia, España y Nueva Zelanda por mencionar sólo algunos. Sin embargo, para 2015 se espera que todos los documentos de viaje sean biométricos.³³ Esta base de datos permite a los oficiales de inmigración y control fronterizo verificar la validez de un documento de viaje.³⁴

Como se mencionó con anterioridad, Interpol regula el intercambio de información contenida en sus bases de datos en relación con los países miembros. Esta regulación se da a través de la utilización de tres estándares diseñados especialmente por Interpol en los métodos de procesamiento de información, en los *loci*³⁵ y en los sistemas de intercambio de información.³⁶

Por tanto, Interpol ha desarrollado normas internas con relación a las condiciones y procedimientos básicos sobre la información procesada de conformidad con el artículo 2 de la Constitución y Regulaciones Generales de Interpol.³⁷

a. Estandarización de los métodos de tratamiento de información

El “Reglamento sobre el tratamiento de información con fines de cooperación internacional en materia policial”,³⁸ las “Disposiciones de implementación sobre

³³ Mandato establecido por la Organización de Aviación Civil Internacional en el Doc 9303, Documentos de viaje de lectura mecánica, Parte 1, Pasaportes de Lectura Mecánica, vol. 1, Pasaportes con datos de lectura mecánica almacenados en formato de reconocimiento óptico de caracteres de 2006. http://www.icao.int/publications/Documents/9303_p1_v1_cons_es.pdf (9 de diciembre de 2012).

³⁴ Bases de datos <http://www.interpol.int/en/Internet/INTERPOL-expertise/Databases> (30 de noviembre de 2012). La traducción es nuestra.

³⁵ En términos simples, el *loci* es el plural de *locus* que esto a su vez significa la posición específica de un gen sobre un cromosoma.

³⁶ Interpol participa activamente en comités de estándares internacionales, especialmente en áreas relativas al ADN forense y otras características biométricas, como por ejemplo en la Red Europea de Institutos de Ciencia Forense (ENFSI por su acrónimo en inglés), <http://www.enfsi.eu/index.php> (30 de noviembre de 2012), y la Organización Internacional de Estandarización (ISO por su acrónimo en inglés), <http://www.iso.org/iso/home.html> (30 de noviembre de 2012).

³⁷ Para profundizar más sobre la Constitución de Interpol consúltese <http://www.interpol.int/en/About-INTERPOL/Legal-materials/The-Constitution> (30 de noviembre de 2012).

³⁸ *Rules on the processing of information for the purposes of international police co-operation* fueron reformadas

el Reglamento para el tratamiento de la información con fines de cooperación internacional en materia policial”³⁹ y el “Reglamento que rige el acceso de las bases de datos y plataformas de telecomunicaciones de Interpol por parte de organizaciones intergubernamentales”⁴⁰ son los tres principales documentos que regulan los métodos por los cuales la información es recolectada, almacenada, analizada e intercambiada por Interpol.

La estandarización incluye los fines para los cuales se procesa la información,⁴¹ la función de la Secretaría General,⁴² la función de las entidades en el procesamiento de información,⁴³ las bases de datos de Interpol,⁴⁴ el derecho a procesar la información, la confidencialidad de la información, los métodos de seguridad, las condiciones generales para el tratamiento de la información,⁴⁵ procedimiento general para el tratamiento de la información, los casos en que la Secretaría General deberá consultar a la fuente de un dato de información, el plazo de la fecha límite y el aplazamiento para justificar la conservación de la información o de un elemento de la información, modificación de la información o de un elemento de la información, el bloqueo o la destrucción de un elemento de la información⁴⁶ y sus consecuencias.⁴⁷ Además, incluye las condiciones y casos en que puede ser un elemento de la información o la información completa suministrada, los procedimientos para suministrar información, la retención de solicitudes de información recibidas y de las comunicaciones internas entre la misma Interpol.

por la Resolución AG/2005/RES15 y entro en vigor el 1 de enero de 2006. Disponible para descargar en archivo de PDF <http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts> (30 de diciembre de 2012).

³⁹ *The Implementing Rules for the Rules on the processing of Information*. Disponible para descargar en archivo de PDF <http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts> (30 de diciembre de 2012).

⁴⁰ *Rules governing access by an Intergovernmental Organization to the INTERPOL telecommunications network and database*. Disponible para descargar en archivo de PDF <http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts> (30 de diciembre de 2012).

⁴¹ La finalidad incluye el tratamiento de información con fines de cooperación internacional en materia policial y para cualquier otro propósito legítimo.

⁴² Esto incluye la solicitud de información y la celebración de acuerdos de cooperación. Consúltense atribuciones en la Constitución de Interpol.

⁴³ Esto incluye el papel de las Oficinas Centrales Nacionales de cada uno de los países miembros, en sus relaciones con las instituciones nacionales autorizadas por cada uno de los países miembros, suministro de información, el control de la información por la fuente de información y uso de la información.

⁴⁴ Esto incluye diferentes categorías de bases de datos, las condiciones para la creación y eliminación de bases de datos.

⁴⁵ Esto incluye las disposiciones relativas a la información personal especialmente clasificada como sensible, las disposiciones relativas a la información extraída, las disposiciones relativas a la información de procesamiento para otros fines legítimos y las disposiciones relativas a la tramitación de notificaciones.

⁴⁶ Esto incluye la iniciativa de una entidad que no sea la fuente de un elemento de información y disposiciones específicas relativas a los anuncios.

⁴⁷ Esto incluye las medidas adoptadas por la Secretaría General y la retención de los elementos de una información.

VANESSA DÍAZ RODRÍGUEZ

En este mismo sentido, Interpol ha desarrollado normatividad interna para el acceso directo, descarga, interconexión, registro directo de información en una base de datos autónoma por parte de una entidad autorizada, por solicitudes de información o en situaciones de urgencia. También, cuenta con disposiciones relativas al seguimiento del tratamiento de la información en los archivos de Interpol y su acceso.⁴⁸

*b. Estandarización del loci*⁴⁹

El conjunto de *loci* establecido por Interpol es utilizado por 185 países miembros para el intercambio de información biométrica. A este estándar se le denomina *Conjunto Normalizado de Loci de Interpol* (ISSOL). Cabe destacar que el ISSOL es idéntico al *European Standard Set* (ESS).⁵⁰ Esta norma se recomienda para facilitar la comparación internacional de ADN, y el requisito mínimo para la inclusión de la base de datos de ADN de Interpol es de 6 de 24 polimorfismos de repeticiones cortas (STR por su acrónimo en inglés)⁵¹ más el marcador del género conocido como amelogenina.⁵²

c. Estándar en los sistemas de intercambio de información

Interpol exhorta a los países miembros a utilizar el sistema operativo “i-link” como sistema operativo principal para ejecutar el portal o la plataforma i-24/7 que permite acceder a las bases de datos en línea,⁵³ las cuales están disponibles a todos los países miembros a partir de la aceptación de ciertos requisitos. En

⁴⁸ *Rules on the Control of Information and access to INTERPOL's files*. Disponible para descargar en archive PDF en <http://www.interpol.int/en/About-INTERPOL/Legal-materials/Fundamental-texts> (30 de diciembre de 2012).

⁴⁹ Interpol, *Manual de Interpol sobre el Intercambio y Utilización de Datos Relativos al ADN, Recomendaciones del Grupo de Expertos en ADN de Interpol*, 2009, Anexo 1: Conjunto Normalizado de Loci de Interpol (ISSOL), p. 90 El documento se encuentra disponible para descarga en archivo PDF a través del buscador del portal de Interpol <http://www.interpol.int/contentinterpol/search?SearchText=DNA&tx=0&ty=0> (30 de noviembre de 2012).

⁵⁰ Los requisitos para el intercambio de ADN son: el uso de la norma internacional ADN (ISSOL –estándar de loci que Interpol recomienda para facilitar la comparación internacional–). Además, la aceptación del documento Carta ADN de Interpol. El país miembro debe utilizar el software de compatibilidad internacional de ADN (© IPISG Lyon), asimismo, debe utilizar el formato de intercambio internacional de datos (Secretaría General. xsd / . xml) y el uso de la red de telecomunicaciones segura (i-24/7).

⁵¹ En términos simples, son marcadores moleculares de ADN no codificante que se repiten consecutivamente de dos hasta seis pares.

⁵² La amelogenina es una proteína utilizada para determinar el sexo de muestras provenientes de seres humanos cuya identidad es desconocida.

⁵³ Excepto en la base de datos de imágenes de abuso sexual infantil y explotación.

el caso de la base de datos de ADN, se requiere la aceptación de la Carta de ADN de Interpol, la utilización del *software* de compatibilidad internacional de ADN y realizar el intercambio con el formato del programa internacional de datos desarrollado por Interpol.

En el caso de huellas dactilares y palmares, las bases de datos de todos los países miembros deben adoptar, y por ende cumplir, la norma ANSI/NIST y el uso de las Directrices de Adquisición del Sistema Automatizado de Identificación de Huellas Dactilares (AFIS por su acrónimo en inglés). En este mismo sentido, los países miembros también deben utilizar el *software* compatible de huella digital internacional o de impresión palmar, así como el sistema de captura de imagen de la huella y el formato de compresión de la huella digital de imágenes.

b) Bases biométricas en materia criminal en Australia, México, Nueva Zelanda y España

En esta sección se dará una breve descripción de las bases biométricas en materia criminal de:

- Australia.⁵⁴
- México.⁵⁵

⁵⁴ El gobierno de Australia, en cooperación con los gobiernos estatales y territoriales, ha establecido un sistema de ADN de investigación criminal. Estas bases de datos criminales son creadas y administradas por CrimTrac, la cual fue establecida el 1 de julio de 2000 con el objetivo de ayudar a la policía, agencias de seguridad y entidades de aplicación de la ley con el fin de facilitar los servicios de intercambio de información y desarrollo de tecnología necesaria para llevar a cabo investigaciones criminales y resolver crímenes. http://www.crimtrac.gov.au/about_us/index.html (30 de noviembre de 2012).

⁵⁵ En 2009, dos legislaciones entraron en vigor: la Ley General del Sistema Nacional de Seguridad Pública, publicada en el *Diario Oficial de la Federación* el 2 de enero de 2009, última reforma publicada en el *Diario Oficial de la Federación* el 14 de junio de 2012 <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGNSP.pdf> (9 de diciembre de 2012) y la Ley de la Policía Federal, nueva ley publicada en el *Diario Oficial de la Federación* el 1 de junio de 2009, última reforma publicada en el *Diario Oficial de la Federación* el 25 de mayo de 2011, con declaración de invalidez de artículos por sentencia de la SCJN, publicada en el *Diario Oficial de la Federación* el 24 junio de 2011, <http://www.diputados.gob.mx/LeyesBiblio/pdf/LPF.pdf> (9 de diciembre de 2012). Estas dos legislaciones establecen los mecanismos para el Sistema de Información Solo Criminal (SISC). La aprobación de estas dos nuevas leyes se obtuvo después de que creó y desarrolló la Plataforma México. Sobre la Plataforma México véase <http://pdba.georgetown.edu/Security/citizensecurity/Mexico/evaluaciones/InformeLabores-plataformamexico.pdf> (9 de diciembre de 2012).

Además, con la cooperación técnica se produjo un intento de mejorar la organización interna de la Secretaría de Seguridad Pública (SSP) para que la "Plataforma México" pudiera desarrollar y cumplir con los objetivos antes mencionados. La cooperación técnica tuvo un costo total (histórico) de \$177.600 Euros: \$148.000 Euros, la contribución del Banco Interamericano de Desarrollo, con cargo a los recursos del Fondo General de Cooperación de España y \$29.600 euros en recursos locales en especie (espacio de oficina, servicios secretariales, comunicaciones, entre otros) <http://www.iadb.org/en/projects/project-description-title,1303.html?id=ME%201094> (9 de diciembre de 2012). Actualmente, bajo el regreso del Partido Revolucionario Institucional (PRI) a la Presidencia con Enrique Peña Nieto, la Secretaría de Seguridad Pública desapareció, sus atribuciones fueron consignadas a la Secretaría de Gobernación.

VANESSA DÍAZ RODRÍGUEZ

- Nueva Zelanda.⁵⁶
- España.⁵⁷

El objetivo es mostrar cómo los países están utilizando estas bases y comparar las experiencias en derecho comparado.

Actualmente existen diferentes criterios para la recolección, acceso, almacenamiento, eliminación de la información y de la gestión de bases de datos biométricas. En principio, cada país cuenta con una legislación especial para la creación de este tipo de bases de datos o bien es la misma legislación penal la que regula las bases biométricas de datos criminales. Por tanto, existen asimetrías entre las bases biométricas de datos criminales.

Por cuestiones metodológicas debemos explicar cuatro cuestiones fundamentales que deben tenerse en cuenta en relación con cualquier base de datos criminal con el fin de proteger el interés público y los derechos humanos: 1) personas incluidas (tipo de sanción); 2) duración de muestras de ADN almacenado; 3) perfiles de acceso a las bases de datos, y 4) protección de privacidad ante el flujo transfronterizo de la información.

- 1) Personas incluidas (tipo de sanción). La inclusión a este tipo de bases de datos generalmente es por el número de años de cárcel (5 años) más que por el tipo de delito. Teóricamente se recomienda que dicha inclusión sea por el tipo de delito, más que el propio crimen, por ejemplo, el robo, el homicidio o abuso sexual. Pareciera que los gobiernos consideran que mientras mayor sea el número de individuos incluidos en las bases de datos, los resultados en la resolución de casos criminales serán mejores.⁵⁸

⁵⁶ En Nueva Zelanda, la legislación sobre investigaciones criminales (*Criminal Investigations Body Samples Amendment Act 2003*) regula al departamento de policía e investigaciones en ciencias ambientales (ESR por su acrónimo en inglés) respecto a los métodos de trabajo para la toma de muestras de ADN y pruebas, incluyendo muestras de referencia para investigaciones específicas y la toma de muestras de individuos para ser incluidos en el Banco de Datos Nacional de ADN. Sin embargo, no existen reglamentos promulgados. <http://legislation.co.nz/act/public/1995/0055/latest/DLM368913.html> (9 de diciembre de 2012).

Por lo que respecta al Banco de Datos Nacional de ADN, está compuesto por dos bases de datos una de sospechosos y el otro sobre los crímenes. Ambas bases de datos se encuentran vinculadas al Banco de Datos Nacional de ADN. <http://www.esr.cri.nz/competencies/forensicscience/dna/Pages/DNAdatabank.aspx> (9 de diciembre de 2012).

⁵⁷ Antes de la aprobación de la Ley Orgánica 10/2007, del 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN no existía regulación alguna respecto al ADN en materia criminal. Esta nueva base de datos de ADN Criminal Único se basa en el Sistema de Índice Combinado de ADN desarrollado por la Oficina Federal de Investigaciones (FBI). Incluye muestras de ADN u otros tejidos corporales tomadas de individuos delincuentes condenados, detenidos, legal, los detenidos, forense, restos humanos no identificados, las personas desaparecidas. Artículos 3 y 4 de la Ley Orgánica 10/2007 reguladora de la base de datos policial sobre identificadores únicos obtenidos del ADN, publicada en el *Boletín Oficial del Estado* No. 242, <http://www.boe.es/boe/dias/2007/10/09/index.php> (9 de diciembre de 2012).

⁵⁸ European Commission, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002

En Australia se permite el registro de ADN de sospechosos, de delincuentes que cometieron delitos graves, de personas convictas y de voluntarios; en Nueva Zelanda se permite el registro de ADN de cualquier sospechoso de cualquier delito que esté sujeto a registro de antecedentes criminales –78 delitos–,⁵⁹ delitos graves de personas convictas y de voluntarios. Por su parte, España autoriza el registro de ADN de convictos, de delincuentes que cometieron delitos graves y de voluntarios. Mientras que en México se permite el registro de ADN no sólo de sospechosos, delincuentes con delitos graves, de convictos y voluntarios; también se incluyen las muestras voz.

Cabe señalar que la recolección del registro de voz por parte del gobierno mexicano también se da de manera aleatoria sin el consentimiento de las personas. Durante llamadas telefónicas los individuos pronuncian palabras “clave” que activan de manera automática el sistema biométrico de identificación de voz, con el objetivo de combatir la corrupción y el secuestro.

- 2) Duración de muestras de ADN almacenado.⁶⁰ La recolección de información biométrica es un tema controversial, pero la preocupación jurídica se incrementa en relación con la temporalidad o duración de las muestras de ADN. Esta preocupación se debe a la posible reutilización o subsecuente uso de la información. Además, es preciso recordar que la información personal debe ser almacenada en relación con el fin solicitado. Pero, sobre todo, las muestras de ADN no deberían ser almacenadas, solamente el registro de la información, en dado caso. No obstante, la mayoría de las legislaciones establece de manera diferente la duración de muestras de ADN almacenado.

Australia, por su parte, establece que la muestra de ADN pueda ser almacenada en el Sistema Nacional de Investigación Criminal de ADN (NCIDD por su acrónimo en inglés) sin establecer un tiempo determinado para su

concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT> (9 de diciembre de 2012), European Commission, Communication from the Commission to the Council and the European Parliament—Towards enhancing access to information by law enforcement agencies (EU information policy) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0429:EN:NOT> (9 de diciembre de 2012), ROMEO CASABONA, CARLOS MARÍA. *Bases de datos de perfiles de ADN y criminalidad*, Cátedra Interuniversitaria, Fundación BBVA—Diputación Foral de Bizkaia de Derecho y Genoma Humano, España, 2002, 237pp.

⁵⁹ De estos 78 delitos en Nueva Zelanda algunos delitos son: el tráfico de migrantes, bombardeos terroristas, financiación del terrorismo, el reclutamiento de miembros de grupos terroristas, participación en grupos terroristas, secuestro, otros crímenes relacionados con aeronaves, delitos relativos a los aeropuertos internacionales, demolición, entre otros. *Criminal Investigations (Bodily Samples) Act 1995*, No. 55 (1 de octubre de 2010) [http://www.legislation.govt.nz/act/public/1995/0055/latest/dlm368904.html?search=ts_act_criminal+investigations+\(bodily+samples\)_resel&tp=1&sr=1](http://www.legislation.govt.nz/act/public/1995/0055/latest/dlm368904.html?search=ts_act_criminal+investigations+(bodily+samples)_resel&tp=1&sr=1) (9 de diciembre de 2012).

⁶⁰ ROMEO CASABONA, CARLOS MARÍA. *op. cit.*

destrucción.⁶¹ En Nueva Zelanda se permite sólo el registro de la información de ADN si el culpable es sospechoso de un delito grave; dicho registro se llevará a cabo en una base de datos de perfiles de ADN.⁶²

En México, la legislación sólo establece el régimen de las bases de datos criminales, pero no cuenta con disposición relativa a la destrucción o retención de muestras, ni supresión de la información contenida en bases de datos penales;⁶³ mientras que en España, el tiempo de destrucción de la muestra de ADN se encuentra estipulado en correlación a la prescripción del delito.⁶⁴

- 3) Perfiles de acceso a las bases de datos. Una de las preocupaciones en cualquier base de datos personal es el perfil de acceso a éstas, y más tratándose de bases de datos biométricas. Por lo que es necesario contar con disposiciones legislativas que regulen el acceso autorizado de las autoridades competentes habilitadas para acceder, buscar y compartir información; así como la regulación de ese acceso, búsqueda y transferencia de información biométrica.

En términos generales, la regulación debe incluir las prácticas y procedimientos de capacitación del personal. Este tipo de regulación es evidente en Australia, México, Nueva Zelanda y España.

En Australia, el Sistema Nacional de Investigación Criminal de ADN establece que sólo el Estado o territorio que suministra el perfil de ADN puede acceder a la información y por ende identificar a la persona a la que pertenece el perfil. Sin embargo, para el Sistema Nacional Automatizado de Identificación de Huellas Dactilares (NAFIS por su acrónimo en inglés) la policía y el Departamento de Inmigración y Ciudadanía (DIAC por su acrónimo en inglés) pueden tener acceso con el fin de gestionar e identificar a los extranjeros en situación ilegal y para apoyar al procesamiento de solicitudes de visado.

En México, bajo la legislación de la policía federal y la ley sobre el sistema nacional de seguridad pública, se establece la creación de la “Plataforma México”. Sin embargo, dichas normas jurídicas sólo establecen que el Centro Nacional de Información es responsable de establecer, gestionar y mantener

⁶¹ Crimes Act 1994 (Cth), s 23YDAE http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s23ydae.html (9 de diciembre de 2012).

⁶² Criminal Investigations (Bodily Samples) Act 1995 No. 55 (1 de octubre de 2010), Public Act, s 2(1), s 7(b)(xiii).

⁶³ <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf> (9 de diciembre de 2012).

⁶⁴ Artículo 9 de la Ley Orgánica 10/2007 reguladora de la base de datos policial sobre identificadores únicos obtenidos del ADN, publicada en el *Boletín Oficial del Estado* No. 242, <http://www.boe.es/boe/dias/2007/10/09/index.php> (9 de diciembre de 2012).

las bases de datos criminales, la red nacional de comunicación y la base de datos de los miembros del personal de seguridad pública.⁶⁵

En Nueva Zelanda, la legislación sobre investigaciones criminales de muestras corporales de 2003 permite el acceso a las siguientes bases de datos por autoridades responsables de migración, administración de extranjeros nacionalizados: Base de Datos Nacional de ADN, Base de Datos de Evidencias Criminales y el Sistema Automatizado de Identificación de Huellas Dactilares.⁶⁶

En España, la Base Única de Datos de ADN Criminal permite el acceso, a nivel nacional por las autoridades nacionales, a los cuerpos de policía de las comunidades autonómicas, y al Centro Nacional de Inteligencia; en el plano internacional contempla a las autoridades judiciales, el fiscal o la policía de terceros países.⁶⁷

En estos países es deseable conocer más acerca de los perfiles de acceso del personal administrativo. Es crucial determinar exactamente quién decide qué datos personales se almacenan, pero también es importante determinar exactamente el cargo jerárquico de quien tiene acceso a esa información y los propósitos para ese acceso.

En las respectivas legislaciones de Australia, Nueva Zelanda y España, la información sobre dichas especificaciones no es clara, y los protocolos o manuales no están disponibles. Sin embargo, cabe destacar el caso de México, en donde esa información está disponible en Internet.⁶⁸

- 4) Protección de privacidad ante el flujo transfronterizo de la información. Como se ha mencionado con anterioridad, las bases biométricas en materia criminal cuentan con un marco legal especial que autoriza al gobierno la recolección, tratamiento de la información biométrica, ya sea ADN, huellas dactilares y demás bases de datos. Sin embargo, la naturaleza jurídica de la información contenida en las bases biométricas en materia criminal es cla-

⁶⁵ Esta plataforma "tecnológica tiene como objetivo coordinar e integrar información de crimen y delitos de las instituciones de seguridad pública a nivel federal, estatal y municipal, a través del desarrollo de varios sistemas: (i) Único de Información Criminal (SUIC); (ii) Único de Administración Penitenciaria (SUAP); (iii) Integral de Operación Policial (SIOP), y (iv) la creación del Centro Nacional de Denuncia (CND) a ser consolidados en una plataforma tecnológica única". Planificación Estratégica del Proyecto "Plataforma México" (ME-11094), Perfil de Cooperación Técnica, 13 de marzo de 2008. Disponible en <http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=1397559> (29 de noviembre de 2012).

⁶⁶ Cuenta con el almacenamiento de más de 430.000 juegos originales de huellas dactilares.

⁶⁷ Artículo 7, incisos a, b y c, de la Ley Orgánica 10/2007 reguladora de la base de datos policial sobre identificadores únicos obtenidos del ADN, publicada en el *Boletín Oficial del Estado* No. 242, <http://www.boe.es/boe/dias/2007/10/09/index.php> (9 de diciembre de 2012).

⁶⁸ Los lineamientos de cada una de las bases de datos pertenecientes a la Plataforma México pueden consultarse en el portal electrónico del Centro Nacional de Información <http://portal.secretariadodejefecutivosnsp.gob.mx/?page=centro-nacional-de-informacion> (9 de diciembre de 2012).

sificada como información personal sensible. Por lo que el marco jurídico de protección recae en la legislación de privacidad o protección de datos personales. Y, por ende, la implementación de dichos sistemas biométricos debe ser bajo el principio de proporcionalidad.

Australia, México, Nueva Zelanda y España cuentan con dicho marco jurídico. No obstante, en Australia, Nueva Zelanda y España es posible encontrar principios de privacidad en relación con los flujos de información biométrica transfronteriza para evitar la divulgación de dicha información al momento de intercambio internacional. Sin embargo, no se encontraron disponibles informes o reportes sobre las normas de privacidad que rigen tanto las bases biométricas criminales como de la información biométrica que es intercambiada a otros gobiernos por cuestiones de cooperación policiaca y/o judicial.

El marco jurídico de protección de datos personales en México es más complicado en comparación con los otros tres países. México cuenta, por un lado, con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y, por el otro, con nueve artículos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental para regular los datos personales en posesión del sector público. Por tanto, el flujo de información biométrica transfronteriza no cuenta con la adecuada protección jurídica.

5. Conclusiones

Es posible identificar que a nivel internacional las bases de datos biométricas criminales empezaron a funcionar antes de que se implementaran a nivel nacional. Lo anterior se debió a la necesidad de realizar un intercambio de información fácil y eficiente para la cooperación policiaca y judicial.

Anteriormente, las bases de datos criminales ordinarias recolectaban características nominales o textuales; actualmente son características biométricas. Las bases de datos criminales no sólo recogen el nombre, fecha de nacimiento, sexo, descripción física, tatuajes o cicatrices y las categorías de delitos, también incluyen características biométricas como el ADN, el rostro, las huellas dactilares, el iris y la voz.

La ley penal nacional o la legislación especial de cada país establece los criterios para la recolección, acceso, almacenamiento, eliminación de la información y la gestión de base de datos. Razón por la cual es posible encontrar asimetrías legislativas y de gestión entre las bases de datos criminales a nivel nacional, lo

cual se ve reflejado en el plano internacional con rubros que no concuerdan, o bien fueron omitidos por no contar con la información. Es decir, no es un problema científico o tecnológico que la información contenida en las bases de datos biométricas a nivel internacional no esté completa o actualizada, es un problema jurídico de origen nacional. Cada país es responsable de la información criminal que envía o intercambia a nivel internacional. Por tanto, los marcos jurídicos nacionales e internacionales de base de datos criminales deben ser negociados con el máximo grado de transparencia y participación de las autoridades de protección de datos personales.

Las bases de datos de Interpol representan el ejemplo a seguir como “mejores prácticas” en la recolección, procesamiento e intercambio de información biométrica que pueda existir.

Ante esta situación, solamente nos resta compartir una reflexión respecto a los motivos o razones por los cuales los gobiernos están recopilando información biométrica, a saber: *a)* para la resolución de crímenes; *b)* para la resolución de crímenes y obtener información biométrica de los individuos, o *c)* para resolver crímenes, obtener información biométrica de los individuos y otro tipo de información que facilite el control de los individuos.

Esta reflexión se desprende de la característica relacionada con la forma en que la información biométrica es recopilada, pues pareciera que los gobiernos recolectan todo tipo de datos biométricos con un subsecuente fin por el que originalmente fueron recolectados. Esto se refleja por la expansión —que está ocurriendo— de las bases de datos biométricas a nivel internacional en materia criminal.⁶⁹

Finalmente, los sistemas biométricos representan un reto no sólo jurídico sino también ético; retos en los que la comunidad internacional está sumergida desde hace tiempo y que países como Australia, México, Nueva Zelanda y España deben enfrentar para brindar el mejor equilibrio ético-jurídico entre los sistemas biométricos y los derechos de la privacidad y protección de datos personales. ■

⁶⁹ A través de estándares se facilita la interoperabilidad de sistemas biométricos. El más reciente estándar lanzado en noviembre de 2011 por los Estados Unidos de América es el ANSI/NIST-ITL1-2011. http://biometrics.nist.gov/cs_links/standard/AN_ANSI_1-2011_standard.pdf (9 de diciembre de 2012).