EL EJERCICIO DE LOS DERECHOS ARCO ANTE EL FLUJO TRANSFRONTERIZO DE INFORMACIÓN BIOMÉTRICA*

Vanessa DÍAZ**

SUMARIO: I. *Introducción*. II. *Información biométrica y su protección jurídica*. III. *Despliegue de sistemas biométricos en un Estado constitucional*. IV. *El ejercicio de los derechos ARCO ante el flujo transfronterizo de información biométrica*. V. *Conclusiones*. VI. *Bibliografía*.

I. INTRODUCCIÓN

Las Tecnologías de la Información y Comunicación (TIC) están revolucionando la forma en la obtención, procesamiento y generación de datos. Uno de los avances más importantes de las TIC ha sido la capacidad de recopilar, almacenar, procesar e intercambiar información biométrica, facilitando el flujo de datos biométricos no sólo a nivel nacional sino también internacional.

Si bien existen grandes ventajas tecnológicas impulsadas por esta revolución digital, lo cierto es que la implementación de la tecnología biométrica genera una serie de retos, desafíos y problemas jurídicos que deben explorarse en su totalidad.

Nuestro estudio se centra en el pleno ejercicio de los derechos de acceso, rectificación, cancelación y oposición, también llamados derechos ARCO, en el flujo transfronterizo de la información biométrica. Para ello, analiza-

* Este artículo forma parte del proyecto de investigación de tesis doctoral sobre *Transborder Biometric Information Flow: Legal Challenges to Personal Privacy and the Need for Public Debate.* Realizado con becas del Consejo Nacional de Ciencia y Tecnología (Conacyt), el Instituto de Ciencia y Tecnología del Distrito Federal y el apoyo del Institute for the Study of Social Change de la Universidad de Tasmania.

** Académica del Instituto de Investigaciones Jurídicas de la UNAM y University Associate de la Facultad de Derecho de la Universidad de Tasmania.

remos los sistemas biométricos regionales existentes: en Europa, el Sistema de Información de Schengen (SIS) y EURODAC; y, en el foro Asia-Pacífico de Cooperación Económica (APEC), la Tarjeta de Viajes de Negocios de APEC.

Ante la falta de acuerdo internacional sobre la implementación de sistemas biométricos, la investigación revela que la comunidad internacional utiliza los acuerdos internacionales y las leyes nacionales en materia de protección de datos personales para regular el flujo transfronterizo de información biométrica. Sin embargo, las diferencias normativas en materia de protección de datos personales hacen suponer la existencia de lagunas jurídicas para el efectivo ejercicio de los derechos ARCO en las diferentes jurisdicciones a nivel internacional.

Este artículo se encuentra dividido en cinco secciones; en la primera se introduce el objeto de estudio, en la segunda se establece la información biométrica como bien jurídico tutelado por los derechos de la privacidad y protección de datos personales, en la tercera se aborda el despliegue de sistemas biométricos, en la cuarta se analizan los sistemas biométricos regionales de Europa y en el foro Asia-Pacífico de Cooperación Económica (APEC), con el objetivo de identificar el ejercicio de los derechos ARCO ante el flujo de información biométrica y, finalmente, en la quinta se desarrollan las conclusiones.

II. Información biométrica y su protección jurídica

No existe una definición unívoca sobre el término biometría o biométrico en sentido estricto. La doctrina se divide al clasificarla como ciencia o técnica;[1] sin embargo, desde una perspectiva científica[2] la definición de la

[1] Al analizar la literatura especializada de la materia, ésta 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, 1997. *Cfr*. Sokal, Robert y James, Rohlf, *Biometry*, 3a. ed., W.H. Freeman, 2003. *Cfr*. Sokal, Robert y James, Rohlf, *Introduction to Biostatistics*, W.H. Freeman, 1973. *Cfr*. Zhang, David D., *Automated Biometrics Technologies and Systems*, Kluwer Academic Publishers, 2000.

[2] 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", *International Review of Law, Computers & Technology*, núm. 13, s. v., pp. 337-363; *Cfr*. Mather, Kenneth y Jinks, John L., *Biometrical Genetics. The Study of Continuous Variation*, Cornell University Press, 1971.

biometría se desarrolla a través de la estadística o la informática. Mientras que quienes la explican cómo técnica o método la abordan desde diferentes campos de la ciencia: biología, agronomía, medicina, etcétera. Sin embargo, actualmente la biometría es utilizada como método estadístico de adquisición de conocimiento, y a través de la observación y la experimentación describe los fenómenos naturales; no obstante, no logra explicar los fenómenos de la naturaleza por sí misma.[3]

Por tanto, el término "biometría" hace referencia a las técnicas y sistemas automatizados de identificación (reconocimiento) y/o verificación (autenticación) de los individuos con base en características específicas, únicas e intransferibles. Es así como se puede establecer la definición de datos biométricos como: *todas aquellas características fisiológicas y morfológicas que nos identifican como individuos únicos*. Cabe señalar que, dentro de las características físicas se encuentran el reconocimiento del iris, de la mano, de las huellas dactilares, del rostro, entre otras. Mientras que en las características de comportamiento se encuentran el reconocimiento de la voz, caminar, firmar, teclear, etcétera.

Ahora bien, existen autores, como Begoña Martínez Jarreta, que consideran a estas características también como inalterables;[4] no obstante, nosotros no compartimos esa percepción de las características biométricas. Ya que existen algunos datos biométricos que pueden ser alterados por el solo transcurso del tiempo o bien por enfermedades, es el caso del glaucoma, enfermedad del ojo que incrementa la presión intraocular impactando directamente el iris.

Es importante destacar que la información biométrica es el resultado directo de las diferencias individuales que existen en el desarrollo anatómico del cuerpo. La información biométrica ha sido asociada a las técnicas de identificación y verificación que se utilizan para incrementar los sistemas de seguridad.[5]

Por ende, la definición normativa de información personal deberá estar conformada por aquellos datos o referencias que dan cuenta no sólo de la vida de un sujeto, es decir, que informan sobre sus transacciones financieras; su situación familiar o estado civil; su solvencia económica o manejo credi-

---

3 *Cfr*. Hopkins, Richard, "An Introduction to Biometrics and Large Scale Civilian Identification", *op. cit*., *supra* nota 2.

4 *Cfr*. Martínez Jarreta, Begoña, "Biometría (técnico)", en Romero Casabona, Carlos María (dir.), *Enciclopedia de Bioderecho y Bioética*, España, Comares, Fundación BBVA, Instituto Roche, Universidad del País Vasco, Universidad de Deusto, 2013, pp. 257-261.

5 Díaz, Vanessa, "Sistemas biométricos en material criminal: un estudio comparado", *IUS Revista del Instituto de Ciencias Jurídicas de Puebla*, núm. 31, vol. VII, pp. 28-47.

ticio; sus creencias religiosas, políticas; su estado de salud; las ocasiones que ha tenido acceso a alguna institución de salud; los seguros médicos o de vida que ha adquirido; los títulos académicos; las preferencias sexuales; el rango salarial; incluso el historial de antecedentes penales o administrativos, sino también de características fisiológicas y morfológicas.

Ahora bien, la información personal, designada como datos personales o información nominativa, es aquella que revela la identidad de la persona, como los datos biométricos.[6] Por la trascendencia de la información biométrica, un manejo inadecuado o bien una excesiva revelación de cierto dato biométrico, sin que medie la autorización expresa del interesado, da lugar a la violación de la privacidad, y desde luego podría generar estigmatización y, en consecuencia, discriminación.[7]

Aunque no todas las características fisiológicas y morfológicas por sí mismas son datos biométricos "sensibles". En algunos casos, los sistemas biométricos de reconocimiento o de autenticación podrían necesitar dos o más datos biométricos.[8] A lo anterior se le denomina sistemas de combinación biométrica; ejemplos: el tipo de sangre, el factor RH, el peso, la estatura, la distancia entre la nariz y los ojos.[9]

Por tanto, se desprende que, según el 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. Sin embargo, compartir datos biométricos con el objetivo de identificar y verificar a los individuos es información personal sensible.

El derecho de protección de datos personales busca preservar la confidencialidad, en este caso de la información biométrica, tanto en la recopilación, manejo como transmisión. Es decir, el titular de dicha información biométrica debe mantener el control de lo que sobre su persona se ha recabado y lo que se almacena en las bases de datos automatizadas, dando paso con ello al reconocimiento del derecho que se tiene de acceso y control de dicha información personal.

---

6 Muñoz de Alba Medrano, Marcia, "El acceso a la información personal en el nuevo marco jurídico mexicano", en Villanueva, Ernesto y Luna Pla, Issa (eds.), *Derecho de acceso a la información pública, Valoraciones iniciales,* México, UNAM, Atlatl, USAID, Konrad Adenauer, 2005, p. 204.

7 *Idem*.

8 Díaz, Vanessa, "Sistemas biométricos en material criminal: un estudio comparado", *op. cit.*, nota 5, p. 34.

9 *Idem*.

Lo anterior ha obligado no sólo al reconocimiento del derecho de acceso a los datos personales, sino también a la sistematización de la información personal; no obstante, la precisión de dicha regulación no siempre ha sido la adecuada.[10]

III. Despliegue de sistemas biométricos

A nivel nacional, la recolección, el almacenamiento y procesamiento de datos biométricos deben ser considerados cuidadosamente al crear bases de datos. Generalmente, los países deben considerar que la creación de bases biométricas son excepciones o limitaciones al derecho de la privacidad y protección de datos personales de los individuos cuyos datos están contenidos en estas bases de datos. Además, debe garantizarse el pleno ejercicio de los derechos de acceso, rectificación, cancelación y oposición de procesar la información biométrica. La implementación de sistemas biométricos debe equilibrar y conciliar, por un lado, los intereses individuales tales como los derechos humanos y libertades públicas, y, por el otro, los intereses públicos, como la defensa y seguridad pública.

En este sentido, cabe señalar que los sistemas biométricos solamente tienen dos objetivos: la identificación (reconocimiento) y la verificación (autenticación) de los individuos sobre la base de algunas características fisiológicas o morfológicas. 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, el ejemplo más común son las bases criminales. El segundo es para verificar, es decir, autenticar la identidad del individuo, por lo que su funcionamiento está basado en la utilización de un dato comparándolo con el mismo dato almacenado previamente, el ejemplo son las bases migratorias.[11]

Así, se debe considerar que para el desarrollo de sistemas biométricos es fundamental distinguir su objetivo. Es decir, el sistema biométrico va a ser utilizado para identificar o para verificar; puesto que el reconocimiento

[10] Bien señala Marcia Muñoz que el acceso a la información personal en el marco jurídico mexicano es incipiente y deja amplios espacios de interpretación y falta de respuesta jurídica en esta materia. *Cfr*. Muñoz de Alba Medrano, Marcia, "El acceso a la información personal en el nuevo marco jurídico mexicano", en Villanueva, Ernesto y Luna Pla, Issa (eds.), *Derecho de acceso a la información pública, Valoraciones iniciales*, México, *op. cit.*, *supra* nota 6, p. 214.

[11] Díaz, Vanessa, "Sistemas biométricos en material criminal: un estudio comparado", *op. cit.*, nota 5, p. 29.

y la autenticación son actividades totalmente diferentes y para ello algunas características fisiológicas son más apropiadas para la identificación y otras son más útiles para la verificación.[12]

Un ejemplo donde se combinan objetivos de identificación y verificación de individuos a nivel internacional son las políticas migratorias a nivel regional. Globalmente, es casi imposible alcanzar políticas migratorias uniformes y heterogéneas debido a la amplia gama de intereses económicos, sociales y culturales relacionados con inmigración en todo el mundo. Sin embargo, la armonización de las políticas migratorias sobre bases regionales es cada vez más común. En el contexto europeo, el Sistema de Información de Schengen (SIS II) y el sistema EURODAC son ejemplos de políticas de visados comunes armonizadas, en las cuales una visa es válida en cualquier país de la zona Schengen y puede ser emitida por un país para viajar a otro de la misma zona. En el contexto de Asia-Pacífico, la APEC ha creado una tarjeta de negocios llamada ABTC que facilita la entrada a corto plazo a los países miembros participantes. Estas políticas de visados comunes de la región se han desarrollado debido a la confluencia de intereses que estos países tienen en el movimiento de los migrantes a través de sus regiones.

Ahora bien, no existe un tratado o convención internacional que verse sobre la información biométrica como tal, y por ende a nivel internacional su protección recae en documentos internacionales sobre privacidad y protección de datos personales. A nivel nacional, generalmente la regulación recae en las leyes sobre privacidad y datos personales que contemplen la sistematización de la información, pero también el flujo de información nacional e internacional.

A nivel internacional sólo existen los estándares desarrollados por la Organización de Aviación Civil Internacional (OACI) para la elaboración de pasaportes, visas y credenciales o documentos de identidad.[13] En cuestiones criminales o prevención del delito se encuentran los estándares desarrollados por Interol, el Instituto Nacional Estadounidense de Estándares (ANSI, por sus acrónimos en inglés), el Instituto Nacional de Estándares y Tecnología (NIST, por sus acrónimos en inglés), por mencionar algunos.

---

[12] *Cfr*. Boulgouris, Nikolaos V. *et al.*, *Biometrics, Theory, Methods, and Applications*, IEEE y Wiley, 2010; Bolle, Ruud M. *et al.*, *Guide to Biometrics*, Springer, 2003. *Cfr*. Zhang, David D., *Automated Biometrics Technologies and Systems*, *op. cit.*, nota 1.

[13] En este mismo sentido se han desarrollado los: ISO/IEC 19794-5:2005, Information Technology. Biometric Data Interchange Formats. Part 5: Face Image Data- AMENDMENT 1: conditions for taking photographs for face image data (2007) y el ISO (ISO/IEC) 19794-5 Biometric Data Interchange Formats defines a standard data format for digital face images to allow interoperability among face recognition systems, government agencies, and other creators and users of face images.

Estos estándares se caracterizaban por ser disimilares y por ende no ser interoperables entre sí. No obstante, a partir de noviembre de 2011, un nuevo estándar fue elaborado.

El estándar ANSI/NIST-ITL1-2011 permite la interoperabilidad entre los distintos sistemas como bases de datos de inmigración y bases de datos criminales, así como el almacenamiento, transmisión y proceso de datos geográficos (ubicación de posiciones), las imágenes contextuales asociadas y datos de audio y visual.[14]

Este estándar supone un nuevo desafío a mediano plazo, ya que facilita el subsecuente uso automatizado de los datos biométricos y otros tipos de datos personales entre los diferentes organismos de diferentes ámbitos, nacional e internacional. Además, este desafío puede generar otro tipo de retos en materia de protección de datos personales, como el acceso de los datos, su fiabilidad y continuidad de protección jurídica en terceros países. Es posible que la información recopilada para su uso posterior con el nuevo estándar ANSI/NIST-ITL1-2011 puede no ser completa o actualizada. Lo anterior menoscaba el principio de calidad de los datos, en dos formas; por un lado, la recolección de los datos debe ser pertinente y no excesiva, con base en la finalidad que persigue su tratamiento y, por el otro, una vez recolectados los datos deben ser actualizados y mantenerse intactos de forma que respondan con veracidad a la situación actual del titular de los datos.

Cabe mencionar que, el nuevo estándar ANSI/NIST-ITL1-2011 contraviene no sólo el principio de calidad de los datos sino también el de proporcionalidad de los datos; la información personal ha de recolectarse para un propósito específico y sólo se utiliza para ese propósito. La mayoría de los países han incorporado este principio en su legislación nacional. Por tanto, el uso posterior de información automatizado como consecuencia del nuevo estándar violenta los principios de calidad y proporcionalidad de los datos personales.

IV. El ejercicio de los derechos ARCO ante el flujo transfronterizo de información biométrica

Las principales preocupaciones ante el flujo de información biométrica son: el menoscabo a la privacidad, la divulgación de información biométri-

[14] http://www.nist.gov/itl/iad/ig/ansi_standard.cfm, fecha de consulta: 26 de mayo de 2014.

ca, el uso indebido y la falta de consentimiento. Sin embargo, poco se ha discutido sobre el procedimiento o ejercicio de acceso, rectificación, cancelación y oposición de los datos –también conocidos como derechos ARCO– por parte del titular ante organismos o sistemas internacionales.

Es importante destacar que, si bien no todos los sistemas biométricos son físicamente intrusivos, todos los sistemas biométricos pueden menoscabar los derechos de privacidad y protección de datos. La intensificación y diversificación de la tecnología biométrica aumenta los problemas de privacidad a nivel nacional e internacional. Aunado a lo anterior, los avances en la capacidad de almacenamiento de la información personal y la simplificación en el flujo transfronterizo de información biométrica crea desafíos jurídicos sobre la finalidad y el posible uso indebido de información.

Por ello, es importante contar con una adecuada legislación en materia de protección de datos personales a nivel nacional que contemple la continuidad de protección jurídica del dato biométrico y garantice el eficaz ejercicio de los derechos ARCO en el flujo transfronterizo de información biométrica.

En este mismo sentido, a nivel internacional se debe contemplar la uniformidad de procedimientos para ejercer los derechos ARCO en cualquier jurisdicción. Los órganos garantes en materia de privacidad o protección de datos personales deben ser capaces de monitorear adecuadamente el flujo transfronterizo de información biométrica y facilitar el ejercicio de los derechos ARCO de los individuos, sin importar el país de residencia. En la medida de lo posible también deben supervisar la operación, gestión y administración de las bases de datos biométricas.

1. *Sistemas biométricos a nivel internacional*

Hoy en día existen muchos organismos y organizaciones internacionales con diferentes objetivos, pero con roles interrelacionados, como Europol e Interpol, que operan bases de datos criminales biométricas.[15] También hay diferentes sistemas biométricos, con objetivos similares pero diferentes estructuras, que administran la información criminal para fines de migración y de prevención del delito. Esta investigación identificó en Europa dos sistemas biométricos. El primero es la base de datos biométrica EURODAC y la segunda el Sistema de Información Schengen (SIS II), ampliado por la

[15] Díaz, Vanessa, "Sistemas biométricos en material criminal: un estudio comparado", *op. cit.*, nota 5.

Convención de Prüm. Mientras que, en la zona Asia-Pacífico, se identificó la base de datos biométrica de la Tarjeta de Negocios de APEC.

Cabe mencionar que poco se ha discutido sobre la rendición de cuentas de estas organizaciones y sus sistemas de trabajo; cómo se toman y aplican las recomendaciones, o cómo se establecen las especificaciones para las bases de datos biométricos. En esta sección se examina el funcionamiento de estas bases de datos biométricas en cuanto a qué información personal se recopila y cómo se hace esto. Lo anterior tiene el objetivo de establecer cómo se ejercen los derechos ARCO a nivel internacional.

> Sistema EURODAC:[16] En 2000 se estableció, a través del Convenio de Dublín, el sistema EURODAC, para establecer una base de datos europea centralizada de solicitantes de asilo, refugiados y para otros nacionales europeos pero que no pertenecen a la Unión Europea y que son detenidos al cruzar ilegalmente las fronteras en territorio de la UE. Incluye la recolección biométrica de las huellas dactilares, este es un sistema biométrico de identificación (reconocimiento) de individuos.

El Sistema Automatizado de Identificación de Huellas Dactilares (AFIS por sus acrónimos en inglés) de EURODAC fue creado por la empresa Steria. Ahora bien, cada Estado miembro dispone de puntos de acceso nacionales y trabaja directamente con las administraciones nacionales. Las huellas dactilares se comparan con los datos dactiloscópicos transmitidos por otros Estados miembros que ya están almacenados en la base de datos central. Si el sistema EURODAC detecta que las huellas dactilares ya se han recogido y almacenado el solicitante de asilo es re-direccionado al Estado miembro que recolectó y almacenó la información por primera vez.

> Sistema de Información de Schengen (SIS II):[17] Para el funcionamiento del sistema libre de control de las fronteras entre los Estados miembros de la zona Schengen, el SIS II proporciona el sistema de apoyo principal. Contiene una "lista" de las personas que han cometido un delito, falta o está bajo observación judicial. Cabe resaltar que la zona Schengen y la Unión Europea son

[16] Reglamento (CE) núm. 2725/2000 del Consejo, del 11 de diciembre de 2000, relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33081_es.htm, fecha de consulta el 26 de mayo de 2014.

[17] Sistema de Información Schengen, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm, fecha de consulta el 26 de mayo de 2014.

dos zonas diferentes; es decir, que no todos los países miembros de la Unión Europea pertenecen a la zona Schengen. Incluye la recolección de huellas dactilares y fotografías, éste es un sistema biométrico de verificación (autenticación) de individuos.

Los Estados miembros de la zona Schengen se alimentan del sistema de información a través de las redes nacionales que están conectados a un sistema central y complementado por la Red SIRENE,[18] quienes son representantes de la policía nacional y local, agencias de aduanas y el poder judicial. Este sistema fue revisado y ampliado por la Convención de Prüm.[19] La compañía Steria también estuvo a cargo en la segunda generación del SIS II. Su capacidad se incrementó no sólo tecnológicamente, sino también en relación con la información recopilada, almacenada e intercambiada.

Tarjeta de Negocios del Foro de Cooperación Económica de Asia-Pacífico (APEC por sus acrónimos en inglés): con el objetivo de facilitar e incrementar la movilidad de la gente de negocios en la región se creó la tarjeta de negocios ABTC (por sus acrónimos en inglés). Con base en los lineamientos previamente acordados por los Estados miembros del foro Asia-Pacífico, esta tarjeta facilita el intercambio de información a través de un sistema en línea, con el fin de mejorar la movilidad de la gente de negocios en la región. Incluye información de huellas dactilares y rostro, este es un sistema biométrico de verificación (autenticación) de individuos. El sistema aporta información sobre los documentos de viaje (pasaportes) perdidos o robados a la base de datos de Interpol.

Los países miembros son los encargados de la expedición de la Tarjeta de Viajes de Negocios para cumplir los criterios de elegibilidad de tarjetas; estándares de servicio y las normas para fabricar la tarjeta. No se elimina la solicitud de visas al visitar los miembros de APEC. Los pasaportes se mantienen como el principal documento de viaje. El flujo transfronterizo de información biométrica incluye: tramitar el despacho de antemano; recibir la autorización; y solicitar la producción de tarjetas. En los tres sistemas biométricos la transferencia de información biométrica se encuentra encriptada y se destaca que son bases de datos centralizadas.

[18] La Red SIRENE es un sistema utilizado por las autoridades policiales para el intercambio de información de acuerdo con el Convenio de Schengen a efectos de la prevención e investigación de hechos delictivos en la zona Schengen por el SIS II.

[19] Ampliación del Sistema de Información Schengen por Convenio Prüm, http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/jl0005_en.htm, fecha de consulta el 26 de mayo de 2014.

2. *Establecimiento de normas de protección de privacidad y protección de datos personales*

APEC es principalmente un foro para promover la cooperación en la región Asia-Pacífico en los asuntos económicos. Esta organización regional de Asia-Pacífico ha considerado las cuestiones de privacidad en relación con la cooperación económica y ha desarrollado un marco de trabajo para los Estados miembros. El marco de privacidad de APEC no es obligatorio o vinculante para los miembros, pero puede desarrollar políticas y asesorar en cuestiones legislativas a los Estados miembros.

Cabe destacar que el marco de Privacidad de la APEC es un conjunto de documentos que brindan asesoría, la cual no es vinculante y formalmente elaboran directrices para los miembros. En 1998, la APEC consideró dentro de su agenda el tema de vida privada, cuando emitió el Plan de Acción sobre el Comercio Electrónico. Pero no fue sino hasta 2004 que la APEC elabora su Marco de Privacidad, en el que resume los principios de privacidad. Los 21 países miembros voluntariamente pueden o no implementar estos principios en su legislación nacional. En consecuencia, el marco de APEC es opcional y su aplicación no ha sido consistente entre los países miembros.[20]

El Marco de Privacidad de la APEC considera el flujo transfronterizo de datos personales, incluso fuera de la región de APEC, a través del principio de rendición de cuentas.[21] El Marco de Privacidad de la APEC incluye un mecanismo de notificación de la aplicación interna del Marco de Privacidad, las directrices de aplicación internacional (intercambio de información entre las economías miembros) y la cooperación transfronteriza en la investigación y aplicación de la ley. Sin embargo, en el momento de escribir esta investigación ningún informe sobre su aplicación estaba disponible.

En 2007, la APEC emitió un programa piloto para la implementación del Marco de Privacidad, llamado Pathfinder de Privacidad de Datos.[22] Como resultado del Plan de Trabajo Pathfinder de Privacidad, en 2012 la

[20] APEC Privacy Framework (2004), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx, fecha de consulta el 6 de mayo de 2014.

[21] El principio de la rendición de cuentas se estableció por primera vez en las directrices de la OCDE.

[22] El Pathfinder fija objetivos para las empresas y agencias de privacidad.

APEC emitió el Sistema de Reglas de Privacidad Transfronteriza, que es un sistema de certificación voluntario.[23]

En resumen, el Marco de Privacidad de APEC es muy escueto, muy general, típico para la implementación internacional y bastante amplio para la cooperación transfronteriza y aplicación de las leyes de privacidad. Además, el Marco de Privacidad de la APEC no es obligatorio y requiere la legislación interna para ser promulgada. Además, el Marco de Privacidad de la APEC no impone controles estrictos y garantías sobre la privacidad y protección de datos en los países miembros. Por tanto, se puede concluir que el Marco de Privacidad de APEC constituye un marco razonable de directrices, pero requiere desarrollo reglamentario o eficacia normativa a nivel nacional.

En 1981, el Consejo de Europa,[24] influenciado por el trabajo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), desarrolló la primera Convención europea sobre el tratamiento de datos personales y las normas de privacidad y protección de datos: el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (también conocido como Convención 108). El CE es una importante organización regional que se ocupa principalmente de los derechos humanos. La CE incluye una membresía amplia de 47 Estados de Europa, más miembros que la Unión Europea con sus 28 Estados miembros. En 2001, el CE publicó un protocolo con respecto a las agencias de privacidad y los flujos transfronterizos de datos.[25]

El Convenio 108 fortalece los derechos del individuo sobre la protección de datos relativos a las técnicas automatizadas de procesamiento, almacenamiento e intercambio de datos de carácter personal. Sin embargo, surgieron

[23] APEC Sistema de Reglas de Privacidad Transfronteriza (2012), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx, fecha de consulta el 26 de mayo de 2014.

[24] Organización internacional de Estrasburgo que comprende 47 países de Europa. Fue creado para promover la democracia y proteger los derechos humanos y el Estado de derecho en Europa. Para más detalles de los instrumentos jurídicos, http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp, fecha de consulta el 26 de mayo de 2014.

[25] Convención para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, se abrió a la firma el 28 de enero de 1981, ETS núm. 108 (entró en vigor el 1 de octubre 1985), en su versión modificada por el Tratado de Lisboa que modifica el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, abierto a la firma el 15 de junio 1995 (que entró en vigor con posterioridad a la aceptación por todas las Partes), modificado por el Protocolo del Convenio STE núm. 108, abierto a la firma el 8 de noviembre de 2001, ETS núm. 181 (entró en vigor tras la aceptación por todas las Partes).

preocupaciones sobre las medidas de protección en las leyes nacionales en materia del flujo transfronterizo de la información personal, por lo que el CE publicó un protocolo adicional al Convenio 108, que reconoce que los comisionados de privacidad juegan un papel central en la protección eficaz de las personas en los flujos transfronterizos de los datos personales.

Tres recomendaciones son especialmente significativas en el Convenio 108. Las recomendaciones no son vinculantes, pero representan un avance significativo en un intento de crear un marco para el flujo transfronterizo de información biométrica en Europa, ya que abordan cuestiones específicas relativas a técnicas automatizadas para el almacenamiento, el uso y el intercambio de datos personales. Además, responden a las preocupaciones actuales con relación a la privacidad y los principios de protección de datos. Éstos son:

- *Recomendación Núm. R(91)10* sobre la comunicación a terceros de los datos personales en poder de los organismos públicos.[26] Esta recomendación reconoce las tendencias crecientes de procesamiento automático de datos, el almacenamiento y el intercambio de información personal por parte de los organismos públicos y su explotación por las ventajas comerciales por parte del sector privado. Por tanto, esta recomendación establece principios de protección de datos (PPD) sobre medidas de seguridad, con base en el Convenio 108, los cuales se pueden implementar en la legislación nacional.
- *Recomendación CM/Rec(2010)13* sobre la protección de las personas en relación con el tratamiento automatizado de los datos personales en el contexto de la creación de perfiles.[27] Esta Recomendación establece 13 condiciones para la recopilación y tratamiento de los datos personales, los derechos de los titulares de los datos, recursos, seguridad de datos y de las autoridades de supervisión. Sin embargo, las excepciones y restricciones limitando la privacidad individual son muy amplias. Estas excepciones son: la seguridad, la seguridad pública, los intereses monetarios del Estado o de la prevención y represión de infracciones penales.

[26] Recomendación R (91) 10 del Comité de Ministros a los Estados miembros sobre la comunicación a terceras personas de datos de carácter personal en poder de organismos públicos, adoptada el 9 de septiembre de 1991.

[27] Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, adoptada el 23 de noviembre de 2010.

- *Recomendación (74)29* sobre la protección de las personas frente a las bases de datos electrónicas en el sector público.[28] Esta recomendación estableció PPD comunes específicos como guía a los Estados miembros para garantizar una aplicación armonizada y uniforme de estos principios. El objetivo era evitar las asimetrías entre la legislación de protección de los datos introducidos en los Estados miembros.

Las recomendaciones y resolución de la CE, para ser vinculantes, necesitan incorporarse a la legislación nacional. No obstante, estos principios de protección de datos han sido promovidos en toda Europa, en colaboración con la Unión Europea (UE). Muchos miembros han firmado el Convenio 108 y puesto en práctica en sus marcos jurídicos nacionales.

Ahora bien, por lo que se refiere a la UE ha desarrollado un régimen obligatorio para la privacidad y protección de datos. La UE exhorta a los países miembros que adopten el marco jurídico en materia de privacidad y se lleve a cabo una evaluación de la idoneidad de las normas y recomendaciones.[29]

El marco jurídico de la UE incluye distintos tipos de normas jurídicas: convenios, protocolos, directrices, recomendaciones y resoluciones, todas son vinculantes para todos los países miembros. Sin embargo, las Directivas[30] vinculantes más importantes en relación con la protección de los datos emitidos por la UE son la Directiva 95/46/CE[31] (conocida como la Directiva de Protección de Datos), su objetivo es establecer el marco regulatorio transfronterizo y equilibrar los intereses de los individuos y de los

[28] Recomendación R (74) 29 relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público, adoptada el 20 de septiembre de 1974.

[29] Artículo 25.6 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial*, núm. L 281 de 23/11/1995.

[30] La directiva es un acto jurídico que la UE, que normalmente dejan los Estados miembros un cierto margen de maniobra para promulgar las normas que adopte. Folsom, Ralph y Lake, Ralph B. (eds.), European Union Law after Maastricht: a practical guide for lawyers outside the common market, Holanda, Kluwer Law International, 1996, p. 5.

[31] Sobre la protección de la privacidad y protección de datos de la presente Directiva es el texto principal de referencia a nivel europeo. La presente Directiva se aplica a los datos tratados y de almacenamiento en las bases de datos no automatizados y automatizados. Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial*, núm. L 281 del 23 de noviembre de 1995.

intereses públicos para el flujo de datos personales en Europa y la Directiva 2009/136/CE.[32]

La Directiva 95/46/CE prohíbe el flujo de información transfronterizo a los países que tienen regímenes de protección de datos inadecuados (incluidos los miembros europeos). El objetivo de esta prohibición es "asegurar que el flujo transfronterizo de datos personales está regulado de una manera consistente".[33] Para la UE, un régimen adecuado de protección de datos se basa en los siguientes requisitos: a) establecimiento de principios de protección de datos personales como obligaciones impuestas a los que participen en el tratamiento de los datos; b) circunstancias bajo las cuales el procesamiento se puede llevar a cabo, incluyendo la naturaleza de los datos, el objeto, la duración de la operación de tratamiento propuestas, calidad de los datos, las normas de derecho general y sectorial en vigor en el tercer país, normas profesionales, la seguridad técnica y la notificación a la autoridad de control, y c) establecimiento de derechos conferidos a los particulares, incluyendo ser informado sobre el flujo transfronterizo de datos, el acceso a los datos transferidos, a solicitar su rectificación o de oposición a la transferencia en circunstancias específicas.[34]

Estas Directivas son importantes y se han complementado con recomendaciones vinculantes y las resoluciones son compatibles con los sistemas biométricos. Sin embargo, estudios comparativos realizados por la CE han señalado que operativamente las leyes de privacidad y protección de datos dentro de las fronteras de los miembros de la UE tienen asimetrías. Algunos de los países miembros difieren en el alcance de su aplicación de las Directivas y en las funciones y atribuciones de sus órganos garantes de protección

[32] Modifica el marco actual de la UE relativo a las redes y servicios de comunicaciones electrónicas, así como cinco directivas. Estas directrices incorporan un gran avance en la regulación del tratamiento de datos personales y a la protección de la vida privada. En primer lugar, se abordan una serie de cuestiones relativas a los sistemas de procesamiento de datos. En segundo lugar, se han actualizado después de que la Comisión Europea (CE) presentó sus conclusiones sobre la revisión del marco regulador de la UE de las redes y servicios de comunicaciones electrónicas en 2006. Directiva 2009/136/EC del Parlamento Europeo del Consejo del 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) núm. 2006/2004 sobre la cooperación en materia de protección de los consumidores.

[33] Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *op. cit.*, nota 31, artículo 25(1), párrafo 8.

[34] *Ibidem*, artículo 25.

de datos personales. Además, algunos estudios académicos e informes han puesto de manifiesto esta falta de armonización en los marcos jurídicos nacionales.[35]

El marco jurídico de la UE de datos transfronterizos facilita la libre circulación de datos personales entre los miembros europeos. Sin embargo, pueden surgir algunos problemas cuando la información personal fluye fuera de la región de Europa con diferentes enfoques de la regulación que se aplican, ya que los países fuera de esta región deben ajustar sus legislaciones nacionales en el marco jurídico de la UE con el fin de transferir los datos personales legalmente.

3. *Ejercicio de los derechos ARCO*

En el caso de la región de Asia-Pacífico, la APEC estableció que las autoridades nacionales encargadas de supervisar el tratamiento de los datos personales serían las responsables de funcionar como enlaces para que sus ciudadanos puedan ejercer los derechos ARCO. Por tanto, el pleno ejercicio de los derechos ARCO recae en las propias legislaciones sobre protección de datos personales, las cuales deben establecer un órgano especializado para supervisar el flujo transfronterizo de información personal. Estas autoridades deben llenar un formato solicitando la cooperación de la autoridad correspondiente en materia de protección de datos personales, por lo que el individuo no ejerce directamente los derechos ARCO.

En Europa existen dos autoridades diferentes encargadas de supervisar el tratamiento de los datos personales; para el sistema EURODAC el encargado es el Supervisor Europeo de Protección de Datos Personales (SEPD),[36]

---

[35] Korff, Douwe, "EC Study on Implementation of Data Protection Directive 95/46/EC" (2002). Disponible en *http://ssrn.com/abstract=1287667*, consultado el 26 de mayo de 2014; Bygrave, Lee, "Privacy Protection in a Global Context. A Comparative Overview", *Scandinavian Studies in Law*, vol. 47, pp. 319-348; Kuner, Christopher, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future", *Tilbrug Institute for Law, Technology and Society* (2010), http://dx.doi.org/10.2139/ssrn.1689483, fecha de consulta el 26 de mayo 2014; Korff, Douwe, "Comparative Study on Different Approach to New Privacy Challenges, in Particular in the Light of Technological Developments" (2010), http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf, fecha de consulta el 26 de mayo de 2014.

[36] https://secure.edps.europa.eu/EDPSWEB/edps/lang/es/EDPS, fecha de consulta el 26 de mayo de 2014.

mientras que para el Sistema de Información Schengen II el encargado es la Autoridad Común de Control de Schengen (ACC).[37]

El Supervisor Europeo de Protección de Datos Personales (SEPD) tiene la responsabilidad de garantizar que las instituciones y organismos de la UE respeten el derecho de las personas a la intimidad en el tratamiento de sus datos personales. Por tanto, el ejercicio de los derechos ARCO ante anomalías en el tratamiento de datos personales por parte del sistema EURODAC recae directamente al SEPD, para poder ejercerlos se puede presentar una queja electrónica cuyo formato está en su portal de Internet.[38] Tal vez, las únicas dificultades son el idioma y tener conocimientos básicos de navegación en Internet para poder ejercer los derechos ARCO ante el SEPD.

El ejercicio de los derechos ARCO en el Sistema de Información Schengen II es más complejo. La Autoridad Común de Control de Schengen (ACC) es un órgano independiente especializado en protección de datos personales, está compuesto por miembros de cada autoridad de protección de datos personales nacional. La ACC ha elaborado directrices para el ejercicio del derecho de acceso, rectificación y cancelación. La solicitud se rige por el régimen nacional del ciudadano que solicita la información personal. Cabe resaltar que el derecho de acceso a la información personal entre cada uno de los Estados miembros de la zona Schengen se diferencia de una agencia a otra.

Por tanto, en la región de Europa, específicamente en la zona Schengen, el ejercicio del derecho de acceso a la información personal es contradictorio y el ejercicio de los derechos ARCO no es fácil de ejercer plenamente, con los distintos procedimientos y prácticas.

En la zona Schengen a nivel nacional, es decir, entre países miembros, se presentan dos escenarios relacionados con el ejercicio del derecho de acceso a la información personal:

- El primer escenario es cuando algunos regímenes de protección de datos establecen un procedimiento directo para ser seguido por las autoridades que operan las bases de datos biométricas a nivel nacional, cuando se solicita el acceso a la información personal. En este caso, los ciudadanos ejercen sus derechos ARCO al hacer sus

[37] http://schengen.consilium.europa.eu/reports/activity-report.aspx?lang=es, fecha de consulta el 26 de mayo de 2014.

[38] https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Complaints, fecha de consulta el 26 de mayo de 2014.

peticiones directamente a la autoridad encargada de la base de datos biométrica.

- El segundo escenario es cuando los regímenes de protección de datos establecen un procedimiento indirecto para el ejercicio de los derechos ARCO a través de solicitudes presentadas ante una autoridad de protección de datos, un mediador o un órgano específico. Esta situación hace que los ciudadanos no puedan acceder directamente a la información personal debido a que la solicitud se presentó ante el comisionado de privacidad, que luego procede a solicitar la información de la autoridad correspondiente en nombre de los ciudadanos. Muy similar a lo que sucede en la zona APEC.

Cabe resaltar que la mayoría de las personas afectadas por el SIS II son extranjeros. Sin embargo, la forma en que se establecen los derechos y recursos jurídicos pareciera estar dirigidos a ciudadanos de la UE.

Con base en lo anterior, se desprende que solamente en EURODAC es posible el pleno ejercicio de los derechos ARCO mientras que en la zona Schengen y APEC resulta más complicado debido a las asimetrías legislativas en materia de protección de datos personales. La zona Schengen cuenta con 26 legislaciones en materia de protección de datos personales y la APEC con 21.

V. Conclusiones

Las organizaciones regionales no sólo han facilitado la implementación de sistemas biométricos centralizados, sino también han fomentado el flujo transfronterizo de información biométrica para el control de la inmigración, prevención de delitos transfronterizos y combate al terrorismo. Estos tres sistemas biométricos regionales utilizan los estándares o normas técnicas de la OACI. Sin embargo, el hecho de que estos sistemas biométricos regionales sean bases de datos centralizadas plantea una pregunta común acerca de la vulnerabilidad tecnológica y riesgos de privacidad con relación al acceso no autorizado, *hackers* y copias de seguridad. Además, es interesante observar que la misma empresa, Steria, sea la encargada de los dos principales sistemas biométricos en Europa.

El flujo transfronterizo de información biométrica debe realizarse con ética, integridad y coherencia no sólo en términos de información, sino también en el cumplimiento de las prácticas principales de protección de datos personales. Un claro y armonizado marco jurídico sobre protección

de datos personales es esencial para reducir las preocupaciones en esta área. Además, un régimen jurídico adecuado sobre el flujo transfronterizo de información biométrica asegurará no sólo la efectividad sino también la eficiencia técnico-jurídica de protección.

Las funciones de las organizaciones regionales (APEC, CE y la UE) están haciendo esfuerzos para crear un marco jurídico internacional para la implementación de estos sistemas biométricos y la regulación del flujo transfronterizo de la información biométrica. Sin embargo, estos intentos requieren la participación activa de todos los sectores, incluido el gobierno, la industria y los actores sociales. Una estrategia inclusiva y proactiva, así como un debate público más abierto sobre los riesgos técnicos (seguridad) y las limitaciones a las libertades civiles; la promoción de los derechos de privacidad y protección de datos; la transparencia y la rendición de cuentas sobre la gestión de estas bases de datos biométricos nacionales e internacionales centralizadas, son fundamentales para garantizar el efectivo ejercicio de los derechos ARCO.

En contraste con el Marco de Privacidad de APEC y el Convenio 108 del CE, las Directivas de la UE encarnan un marco legal obligatorio. Las directivas obligatorias de la UE establecen un régimen regional e imponen estrictos controles y garantías en materia de protección de datos. El marco jurídico de protección de los datos obligatorios de la UE se extiende a países fuera de la UE, ya que estos países deben tener protecciones equivalentes en materia de protección de datos. El marco jurídico de la UE proporciona un ejemplo de la mejor práctica de la protección de la privacidad y protección de datos y garantiza la eficacia de la reglamentación a nivel nacional, así como el flujo transfronterizo de información biométrica.

Los sistemas biométricos desplegados en Asia-Pacífico y Europa representan desafíos jurídicos donde se hacen evidentes las diferencias y complejidades jurídicas para ejercer los derechos ARCO en su totalidad.

VI. Bibliografía

Ampliación del Sistema de Información Schengen por Convenio Prüm http://europa.eu/legislation_summaries/justice_freedom_security/police_customs_cooperation/jl0005_en.htm.

APEC Privacy Framework (2004), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

———, Sistema de Reglas de Privacidad Transfronteriza (2012), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx.

BOLLE, Ruud M. *et al.*, *Guide to Biometrics*, Springer, 2003.

BOULGOURIS, Nikolaos V. *et al.*, *Biometrics, Theory, Methods, and Applications*, IEEE y Wiley, 2010.

BYGRAVE, Lee, "Privacy Protection in a Global Context. A Comparative Overview", *Scandinavian Studies in Law*, vol. 47.

CONVENCIÓN PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, se abrió a la firma el 28 de enero de 1981.

DÍAZ, Vanessa, "Sistemas biométricos en material criminal: un estudio comparado", *IUS Revista del Instituto de Ciencias Jurídicas de Puebla*, núm. 31, vol. VII.

DIRECTIVA 2009/136/EC del Parlamento Europeo del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) núm. 2006/2004 sobre la cooperación en materia de protección de los consumidores.

DIRECTIVA 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial*, núm. L 281 del 23 de noviembre de 1995.

FOLSOM, Ralph y LAKE, Ralph B. (eds.), *European Union Law after Maastricht: a practical guide for lawyers outside the common market*, Holanda, Kluwer Law International, 1996.

HOPKINS, Richard, "An Introduction to Biometrics and Large Scale Civilian Identification", *International Review of Law, Computers & Technology*, núm. 13.

KING, Robert C. y STANSFIELD, William D., *A Dictionary of Genetics*, Oxford University Press, 1997.

KORFF, Douwe, "Comparative Study on Different Approach to New Privacy Challenges, in Particular in the Light of Technological Developments" (2010), http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf.

———, "EC Study on Implementation of Data Protection Directive 95/46/EC" (2002), http://ssrn.com/abstract=1287667.

KUNER, Christopher, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future", *Tilbrug Institute for Law, Technology and Society*, 2010, http://dx.doi.org/10.2139/ssrn.1689483.

MARTÍNEZ JARRETA, Begoña, "Biometría (técnico)", en ROMERO CASABONA, Carlos María (dir.), *Enciclopedia de Bioderecho y Bioética*, España, Comares, Fundación BBVA, Instituto Roche, Universidad del País Vasco, Universidad de Deusto, 2013.

MATHER, Kenneth y JINKS, John L., *Biometrical Genetics. The Study of Continuous Variation*, Cornell University Press, 1971.

MUÑOZ DE ALBA MEDRANO, Marcia, "El acceso a la información personal en el nuevo marco jurídico mexicano", en VILLANUEVA, Ernesto y LUNA PLA, Issa (eds.), *Derecho de acceso a la información pública, Valoraciones iniciales*, México, UNAM, Atlatl, USAID, Konrad Adenauer, 2005.

RECOMENDACIÓN CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, adoptada el 23 de noviembre de 2010.

RECOMENDACIÓN R (74) 29 relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público, adoptada el 20 de septiembre de 1974.

RECOMENDACIÓN R (91) 10 del Comité de Ministros a los Estados miembros sobre la comunicación a terceras personas de datos de carácter personal en poder de organismos públicos, adoptada el 9 de septiembre de 1991.

REGLAMENTO (CE) núm. 2725/2000 del Consejo, del 11 de diciembre de 2000, relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín.

SISTEMA DE INFORMACIÓN SCHENGEN, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm.

SOKAL, Robert y JAMES, Rohlf, *Biometry*, 3a. ed., W.H. Freeman, 2003.

——— y JAMES, Rohlf, *Introduction to Biostatistics*, W.H. Freeman, 1973.

ZHANG, David D., *Automated Biometrics Technologies and Systems*, Kluwer Academic Publishers, 2000.