RPD
REVISTA DEL POSGRADO EN DERECHO DE LA UNAM
NUEVA ÉPOCA, NÚM. 10, ENERO-JUNIO 2019

La autenticación y verificación de la identidad a través de información biométrica como paradigma del tratamiento de datos personales en México

The authentication and verification of identity through biometric information as a paradigm of the treatment of personal data in Mexico

Tábata Andrea Romero Cerdán[1]

Resumen: El rápido progreso de las tecnologías biométricas y su aplicación generalizada en el sistema financiero mexicano, precisan de un estudio pormenorizado desde el punto de vista de la protección de datos personales. Dado que los datos biométricos han sido incluidos de manera incipiente en la normativa mexicana, en el presente artículo, se analiza su régimen jurídico desde el contexto europeo, abordándose además, las ventajas e inconvenientes que puede suponer la implantación de sistemas de almacenamiento masivo de información biométrica, a la luz de los derechos fundamentales de los individuos. Finalmente, apuntaré posibles soluciones que supongan una menor intrusión contra los derechos de los usuarios y clientes de las instituciones financieras.

Palabras Clave: *Tratamiento de datos personales, datos biométricos, Reglamento Europeo de Protección de Datos, Sistema Financiero Mexicano, protección de datos personales.*

Abstract: The rapid progress of biometric technologies and their widespread application in the Mexican financial system, require a detailed study from the point of view of the protection of personal data. Given that biometric data have been incipiently included in the mexican regulations, in this article, its legal regime is analyzed

[1] Posdoctoranda y becaria CONACYT para realizar estancia de investigación en el Programa de Posgrado en Derecho de la UNAM. Doctora en Derecho por la Benemérita Universidad Autónoma de Puebla. Correspondencia: <tabataandrea@hotmail.com>. ORCID: <https://orcid.org/0000-0002-8493-2432>.

Fecha de Recepción: 16 de noviembre de 2018; Fecha de Aprobación: 18 de marzo 2019.

from the European context, also addressing the advantages and disadvantages that may involve the implementation of massive information storage systems biometric, in light of the fundamental rights of individuals. Finally, I will point out possible solutions that involve less intrusion against the rights of users and customers of financial institutions.

KEYWORDS: *Processing of personal data, biometric data, European Regulation of Data Protection, Mexican Financial System, protection of personal data.*

SUMARIO: I. Datos biométricos: aproximaciones previas; II. Regulación jurídica del tratamiento de datos biométricos en la Unión Europea; III. El tratamiento de datos biométricos en el Sistema Financiero Mexicano; IV. Criterios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para el tratamiento de datos biométricos; V. Tratamiento de datos biométricos: seguridad financiera vs protección de datos personales; VI. Conclusiones; VII. Fuentes de información.

I. DATOS BIOMÉTRICOS: APROXIMACIONES PREVIAS

En la literatura reciente, se refiere a los datos biométricos como las características físicas, fisiológicas, morfológicas, de comportamiento y rasgos de personalidad distintivas de cada persona, que "permiten distinguir ciertas singularidades que concurren en los aspectos analizados y que, resultando imposible la coincidencia en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión".[2] Por otra parte, algunos especialistas consideran que los datos biométricos son una categoría más de los llamados datos sensibles, en el entendido que el uso indebido de éstos, podrá generar discriminación, afectado la esfera más íntima de su titular.

[2] Aparicio Salom, Javier, *Estudio Sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Navarra, Editorial Aranzadi, 2000, p. 54.

Establecido lo anterior, los datos biométricos se entenderán en sentido restringido como datos sensibles,[3] en tanto que en el contexto más amplio, como características físicas[4] o de personalidad,[5] que mediante un procesamiento técnico de reconocimiento, al distinguir las particularidades únicas de cada persona, permiten autenticar su identidad, haciendo imposible resultados coincidentes entre dos individuos.

Surge entonces precisar que el proceso de autenticación puede realizarse a través de dos modos diferentes de reconocimiento: identificación y verificación. En la verificación, se autentica la identidad del usuario mediante la comparación de un dato con el mismo dato previamente almacenado, de tal forma que se verifica que la identidad proporcionada corresponda con la realidad. En la identificación, se averigua la identidad de un sujeto a través de la búsqueda que se realice en una base de datos.[6]

Aquí, es de particular relevancia que los datos biométricos no constituyen los únicos datos o sistemas que permiten la identificación y verificación de los seres humanos. A lo largo de la evolución

---

[3] De acuerdo con el criterio del INAI (en adelante, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales), pese a que los datos biométricos no se encuentran expresamente previstos en la definición de datos sensibles que señala la Ley de la materia, podrán considerarse de esta naturaleza cuando: a) se refieran a la esfera más íntima de su titular; b) su utilización indebida pueda dar origen a discriminación, o c) su uso ilegítimo conlleve un grave riesgo para su titular. *Vid.* INAI, *Guía para el tratamiento de Datos Biométricos*, Ciudad de México, 2018, p. 19. Disponible en: <http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf> (Fecha de consulta: 15/09/2018).

[4] Entre los datos biométricos relativos a características físicas y fisiológicas más utilizados están: la huella dactilar, la retina y el iris del ojo, la palma de la mano, los rasgos del rostro, la exploración del patrón venoso de la muñeca y la composición química del olor corporal.

[5] Entre los datos biométricos de comportamiento encontramos la firma, la voz y la forma de caminar.

[6] Neira Orjuela, Fernando, "Biometría y control migratorio en América Latina" en *Cuadernos de H Ideas*, Argentina, Vol. 9, Núm. 9, diciembre 2015, p. 2.

tecnológica, se han implementado diversos procesos de autenticación. Por ejemplo, es común que al momento de registrar una cuenta en plataformas de correos electrónicos, se solicite información que solo el usuario conoce. De este modo, en caso de que se olvide la contraseña de acceso, se podrá verificar la identidad de la persona registrada, a través de la respuesta a preguntas concretas almacenadas con antelación.

Pero más allá del proceso de verificación e identificación, los datos biométricos se constituyen como un paradigma de seguridad, al proporcionar información de naturaleza indubitable. Los datos biométricos, no se refieren a información sobre una persona; más bien otorgan información intrínseca de ella misma, que no puede modificarse por voluntad propia. Esta propiedad de perpetuidad, hace que la información no puede ser sustituida, modificada o remplazada y no sufre afectaciones por el transcurso del tiempo.

Por esta tendencia del uso de la tecnología como fuente infalible de información para realizar operaciones y transacciones seguras, los datos biométricos se configuran como una herramienta cada vez más utilizada por los Estados como medio de identificación inequívoca de las personas. De ello, se desprende que a partir del año 2017, las instituciones financieras en México, recolectan datos biométricos como medida de verificación de la identidad de los usuarios y clientes de la banca.[7]

---

[7] El 29 de agosto de 2017, la Comisión Nacional Bancaria y de Valores (en adelante, CNBV) publicó en el Diario Oficial de la Federación (en adelante, DOF), una serie de cambios a la Circular Única de Bancos que buscan combatir el robo de identidad dentro del sector bancario. Estos cambios incorporan y regulan el uso de datos biométricos (huella dactilar, principalmente) para la autenticación de los usuarios de la banca. *Vid.* Resolución que modifica las Disposiciones de Carácter General aplicables a las Instituciones de Crédito, DOF, 29/08/2017. Disponible en: <https://www.cnbv.gob.mx/Resoluciones%20Modificatorias/100a.%20Resoluci%C3%B3n%20modificatoria%20CUB.pdf> (Fecha de consulta: 22/05/2018).

II. Regulación jurídica del tratamiento de datos biométricos en la Unión Europea

En los últimos años, el uso masivo e indiscriminado de los datos biométricos en la vida cotidiana de los individuos, ha convertido su regulación en un verdadero reto jurídico. En virtud de ello, se antoja el análisis del Reglamento Europeo de Protección de Datos, ya que todo estudio de derecho comparado, ofrece una herramienta indispensable para toda investigación jurídica y fundamento elemental para las transformaciones del marco jurídico nacional.

El pasado 27 de abril de 2016, el Parlamento Europeo y del Consejo, aprobó el Reglamento (UE) 2016/679 (en adelante, RGPD) con el que se le otorga a algunos datos personales, la calidad de especiales, por concebir que dada su naturaleza, requieren de una protección particular.

A partir de esta idea, se puede encontrar en la normativa Europea el concepto jurídico de datos biométricos, definidos como los "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".[8]

Al planteamiento expuesto, resulta adecuado resaltar lo señalado en el apartado 1 y 2 del artículo 9 del RGPD:

> Queda prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera uní-

---

[8] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Vid.* Artículo 4, inciso 14). Disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf> (Fecha de consulta: 28/06/2018).

voca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados; b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social; c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados; e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial; g) el tratamiento es necesario por razones de un interés público esencial, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado; h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social; i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria

> y de los medicamentos o productos sanitarios, y j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

A su vez, el RGPD prevé la obligatoriedad a cargo de los responsables del tratamiento, de realizar una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, […]".[9]

Conscientes del impacto y gravedad del tratamiento de datos biométricos, los responsables deberán con base en una evaluación objetiva, ponderar el riesgo y alcance que implica su recolección, almacenamiento y transferencia, a fin de determinar si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto. Sobre este punto es menester precisar que se hablará de riesgo, cuando exista la posibilidad de que se genere un daño, en tanto que el riesgo alto, implica una hipótesis en la que el tratamiento de datos personales puede causar una vulneración grave de los derechos y libertades de las personas.

Ante este escenario, el tratamiento de datos biométricos actualiza la hipótesis del riesgo alto, ya que a partir de éstos podrá conocerse de una persona, su origen racial, género, datos filatorios, entre otros; cuyo uso indebido podrá significar una vulneración grave a sus derechos fundamentales. En suma, de conformidad con la normativa española, el tratamiento de datos biométricos que tenga como fin identificar inequívocamente a una persona, esta expresamente prohibido, sin embargo, si su uso se encuadra en alguno de los supuestos de excepción que el mismo Reglamento señala, deberá realizarse invariablemente la evaluación de impacto correspondiente, la cual deberá incluir entre otros: a) una descripción

---

[9] *Ibidem*, artículo 35.

sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento y, b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.[10]

1. Legitimación del tratamiento de datos biométricos

Como se desprende del texto anterior, los responsables del tratamiento de datos biométricos deberán precisar en la evaluación de impacto, la base de legitimación del tratamiento. Tal obligación privilegia el principio en el que se sustenta todo derecho a la protección de datos personales: la licitud. Ello significa que en primer lugar, el responsable deberá acreditar el consentimiento del interesado; en segundo lugar, que el tratamiento se realice en apego al consentimiento otorgado o bien de conformidad con alguna base legítima establecida en el RGPD y, en tercer lugar, en caso de que el tratamiento se funden en el interés legítimo perseguido por el responsable, éste deberá privilegiar en todo momento los derechos de las personas, además de tomar en cuenta las expectativas razonables de aquellos que pudieran resultar afectadas por el tratamiento.

2. Evaluación de la necesidad y la proporcionalidad

El RGPD obliga a los responsables a realizar una evaluación de la finalidad con la que los datos son tratados a fin de determinar su necesidad y proporcionalidad. Aquí, baste mencionar que conforme a lo señalado en considerando 39 del propio dispositivo normativo:

> Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos

[10] *Ibidem*, artículo 35.7.

> personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. […] Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.[11]

Para realizar una adecuada evaluación de impacto en materia de protección de datos personales en consistencia con las disposiciones previstas en el RGPD, el Grupo "Protección de Datos" del Artículo 29, elaboró una serie de directrices para la aplicación de los principios de necesidad y proporcionalidad.[12] Este grupo de trabajo, considera que la necesidad se acredita cuando la finalidad con la que

[11] *Ibidem*, considerando (39).

[12] *Vid*. Grupo "Protección de Datos" del Artículo 29, *WP 248 rev.01: Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE)*

se realiza el tratamiento de datos personales no puede conseguirse por otros medios, en tanto que la proporcionalidad, se comprobará a través de tres análisis: el de necesidad, el de idoneidad y el de proporcionalidad en sentido estricto. La convergencia de éstos tres, permitirá a los responsables del tratamiento ponderar los derechos y libertades en juego, para determinar la necesidad y proporcionalidad de la medida.

A partir de esta idea, nos resulta necesario mencionar que el ex Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo de la Organización de las Naciones Unidas, Martin Scheinin, señaló en su informe del año 2009 que en determinadas circunstancias, podría legitimarse el uso de información biométrica para la identificación de sospechosos por actos de terrorismo ya que su recolección atiende al interés general; sin embargo, la centralización de información en bases de datos, incrementa los riesgos para la seguridad, dejando a los individuos vulnerables ante situaciones de criminalización ilícita de individuos o exclusión social. Además, los datos biométricos favorecen intrusiones en la vida de las personas de carácter permanente, ya que los detalles físicos y biográficos de las personas son inmutables y no pueden revocarse. A este escenario, se adicionan los acontecimientos de ventas de datos de información que se traducen en delitos de extorsión, vigilancia, chantaje y lucro.

En resumen, conforme a lo sustentado por el ex Relator, el tratamiento de datos personales resulta una medida innecesaria ya que la finalidad que persigue puede agotarse con mecanismos menos intrusivos y puede lograrse razonable por otros medios; asimismo, es desproporcional, ya que no es ponderada o equilibrada con los derechos fundamentales, pudiendo causar daños irreparables.

2016/679, Bruselas, 2017. Disponible en: <https://www.aepd.es/media/criterios/wp248rev01-es.pdf> (Fecha de consulta: 18/09/2018).

Lo dicho hasta aquí, nos lleva a concluir que el RGPD pretende evitar cualquier tratamiento de datos biométricos que identifique inequívocamente a una persona, motivo por el cual, resulta relevante que en los siguientes apartados se aborde el paradigma que representan los datos biométricos en el sistema financiero mexicano.

III. El tratamiento de datos biométricos en el Sistema Financiero Mexicano

Con la finalidad de fortalecer los procedimientos que utilizan las instituciones de crédito para identificar a las personas que contraten con ellas productos, servicios o realicen operaciones en ventanilla, el 29 de agosto de 2017, la CNBV publicó en el DOF, disposiciones para la identificación de sus usuarios y/o clientes.[13] En virtud de lo anterior, se reformó la denominación del Capítulo II relativo a la *Integración de Expedientes de Crédito* de las Disposiciones de Carácter General aplicables a las Instituciones de Crédito (en adelante, DCGIC) para quedar como *Integración de Expedientes de Crédito y datos de identificación de los clientes,* adicionando entre otros, los artículos 51 Bis a 51 Bis 4, por los cuales, se faculta a las Instituciones de Crédito a realizar una autenticación en línea de las huellas dactilares, así como a conformar una base de datos biométricos.

Con relación a las personas físicas que pretendan celebrar contratos para realizar operaciones activas, pasivas, de servicios, soliciten medios de pago o en su caso, realicen operaciones de retiro en efectivo y transferencias de recursos, las Instituciones Crediticias serán responsables de "autenticar en línea que la huella dactilar que se obtenga de la persona física que presenta la credencial para

[13] Resolución que modifica las Disposiciones de Carácter General aplicables a las Instituciones de Crédito. *Op. Cit.,* nota 6.

votar, coincide al menos en un noventa y ocho por ciento con los registros del Instituto Nacional Electoral".[14]

En relación con lo anterior, cuando el Instituto Nacional Electoral no pueda responder a las solicitudes de verificación en línea, las Instituciones de Crédito podrán celebrar los contratos correspondientes, siempre y cuando dispongan de los dispositivos electrónicos necesarios para recabar y almacenar en ellos la información que se requiera para realizar la verificación con posterioridad.

En este sentido, las DCGIC prevén la conformación de una base de datos de huellas dactilares como mecanismo alterno de verificación. Para ello, la Instituciones deberán: almacenar en una base, los datos de la credencial para votar de sus clientes; capturar las huellas dactilares de los empleados y directivos que tendrán a su cargo la recopilación de datos biométricos, para continuar con la toma de imagen de las crestas papilares de los diez dedos de sus clientes; finalmente deberán verificar en línea la correspondencia de los datos de la credencial para votar con los registros del Instituto Nacional Electoral (en adelante, INE) autenticando la huella dactilar. Este procedimiento se realiza por única ocasión y a partir de entonces, los bancos podrán utilizar esta base de datos para autenticar a sus clientes, sin necesidad de hacer la verificación en línea con los registros del INE.

La referida política de recolección y verificación de datos biométricos, atendió a que la CNBV y las Instituciones de Crédito detectaron la necesidad de fortalecer los procedimientos de identificación de los usuarios con el objetivo de prevenir y/o detectar fraudes como la suplantación de identidad. Por ello, en el caso de retiros y transferencias de recursos de cuentas bancarias, cuando las Instituciones de Crédito determinen procedente no realizar las acciones de verificación y en caso que se presente una situación de suplantación de identidad, éstas deberán asumir los costos de

---

[14] *Ibidem*, artículo 51 Bis 4 inciso b).

las operaciones que no sean reconocidas por sus clientes, así como abonar el monto objeto de reclamación, en un plazo de cuarenta y ocho horas.

Adicionalmente, es importante destacar que las DCGIC prevén la celebración de contratos para la apertura de cuentas bancarias en una modalidad no presencial. Para la identificación remota, la norma señala que los clientes deberán enviar un formulario que entre otros datos, contiene el consentimiento expreso para que su voz e imagen se grabe en el momento en el que la Institución realice una entrevista a distancia en tiempo real. Además, al cliente se le solicitará por una parte, que envíe una fotografía a color de la credencial para votar vigente expedida por el INE y por la otra, que se tome una fotografía en línea utilizando la tecnología que para tales efectos dispongan las Instituciones. Lo anterior, con la finalidad de realizar la autenticación de identidad a través del reconocimiento facial.[15]

Como se ha expuesto, el uso de la huella digital, el reconocimiento facial, la verificación de voz y en general, la captura y recolección de cualquier dato biométrico, se configuran como protocolos de autenticación basados en tecnología, cuyo sustento jurídico se percibe en las políticas de combate a la suplantación de identidad. No obstante, pese a que su formalización se tenía prevista para finales del mes de agosto del año 2018, la CNBV prorrogó el plazo para la aplicación de los controles biométricos, a aquellas Instituciones Bancarias que participaran en la creación de la plataforma única de datos biométricos. Se trata de una base universal, que permitirá verificar la identidad de los usuarios mediante el intercambio de datos e información con el INE, el Sistema de Administración Tributaria (SAT) y la Secretaría de Relaciones Exteriores.[16]

---

[15] *Ibidem*, artículo 51 Bis 6.

[16] Juárez, Edgar, "CNBV arrancará supervisión en línea del sector financiero" en *El Economista*, 19 de junio de 2015. Disponible en: <https://www.eleconomista.

iv. Criterios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para el tratamiento de datos biométricos

Ante el inminente uso de los datos biométricos como mecanismo de autenticación y verificación de identidad, el INAI en su calidad de órgano garante del tratamiento de datos personales y con el objetivo de establecer criterios que garantizaran el tratamiento adecuado de datos biométricos, publicó en marzo de 2018, la *Guía para el tratamiento de Datos Biométricos*.

El documento a que se hace en referencia en el párrafo anterior, presenta una serie de elementos apegados a los principios previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante, LFPDPPP), y en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante, LGPDPPSO), y se configura como un instrumento de observancia obligatoria para la empresas, organizaciones, profesionistas y autoridades que pretendan o traten datos biométricos.

En este sentido, el INAI precisa que un dato biométrico deberá considerarse como un dato personal siempre y cuando de manera directa identifique a su titular, o lo haga identificable a través de la biometría. Continúa precisando que, aunque los datos biométricos no se encuentren señalados expresamente en la LFPDPPP o en la LGPDPPSO, éstos se considerarán sensibles cuando se refieran a la esfera más íntima de su titular, su utilización indebida pueda dar origen a discriminación, o su uso ilegítimo conlleve un grave riesgo para su titular.[17]

Así, el órgano garante resalta que en todos los casos mencionados con antelación, será necesario aplicar políticas afines a los

---

com.mx/sectorfinanciero/CNBV-arrancara-supervision-en-linea-del-sector-financiero-20180619-0154.html> (Fecha de consulta: 22/06/2018).

[17] INAI, *Op. Cit.*, nota 2, p. 19.

principios que rigen el tratamiento de datos personales y realiza las siguientes recomendaciones; a saber:

> Recomendaciones relacionadas con principio de licitud.[18] Conocer la normatividad que en lo específico regula y aplica a la actividad en la que son tratados los datos biométricos y, revisar las atribuciones que facultan al sujeto obligado para tratar datos biométricos, o bien, si su uso está debidamente justificado según la finalidad de la que se trate.
> Recomendaciones relacionadas con el principio de lealtad:[19] Utilizar medios que estén permitidos por la ley; verificar que en el aviso de privacidad se señale de manera expresa el tratamiento de los datos biométricos y, tener especial cuidado en el tratamiento de datos biométrico, a fin de que éste se apegue a lo informado al titular y se privilegie en todo momento sus intereses con relación al uso de sus datos personales.
> Recomendaciones relacionadas con el principio de información:[20] Informar expresamente en el aviso de privacidad que se recabarán datos biométricos, especificando su tipo (por ejemplo, huellas dactilares o iris); cuando los datos biométricos que se traten sean sensibles, señalarlo en el aviso de privacidad; incluir en el aviso de privacidad las finalidades para las cuales serán tratados; cuando se realicen transferencias de datos biométricos, informarlo en el aviso de privacidad y, en caso de que éstas requieran consentimiento, señalarlo; si las finalidades o transferencias de datos biométricos requieren consentimiento, se deberá ofrecer al titular un mecanismo para que pueda otorgar o negar su consentimiento; en el caso del sector público, incluir en el aviso de privacidad las disposiciones normativas que fundamentan el tratamiento de los datos biométricos y tomar en cuenta que, debido a la naturaleza de los sistemas biométricos tratados para fines de reconocimiento, normalmente se llevarán a cabo dos etapas en las que estos datos serán recolectados: la primera, para la creación de las plantillas que serán almacenadas

---

[18] *Ibidem*, p. 23.

[19] *Ibidem*, p. 24.

[20] *Ibidem*, p. 26.

en el sistema biométrico; la segunda, para la comparación de nuevas muestras biométricas con las plantillas almacenadas.

Recomendaciones relacionadas con el principio de consentimiento[21]: Solicitar el consentimiento tácito de los titulares de los datos biométricos, cuando éstos no resulten sensibles, y solicitar el consentimiento expreso y por escrito de los titulares de los datos biométricos, previo a que se recaben, o bien, en el momento en que lo indique la normativa aplicable, cuando éstos resulten sensibles.

Recomendaciones relacionadas con el principio de finalidad:[22] Describir en el aviso de privacidad la o las finalidades para las cuales serán tratados los datos biométricos recolectados; no tratar los datos biométricos del titular para finalidades distintas, que no resulten compatibles o análogas a aquéllas para las cuales fueron recabados, y cuando los datos biométricos que se recaben se consideren sensibles, las finalidades para las cuales se recaben y traten los datos biométricos deberán estar debidamente justificadas.

Recomendaciones relacionadas con el principio de proporcionalidad:[23] Evaluar si la recolección de datos biométricos es necesaria para la finalidad pretendida; priorizar el uso de datos que no sean biométricos para lograrla misma finalidad sin restarle efectividad; obtener y utilizar únicamente los datos biométricos que sean necesarios, adecuados y no excesivos para las finalidades para las que fueron recabados; recolectar y tratar el número mínimo de datos biométricos necesarios para la finalidad para la cual se están recolectando; evitar o limitar al máximo la recolección de datos biométricos que pudieran revelar datos sensibles no necesarios para las finalidades legítimas que se persiguen, y la cantidad de muestras biométricas también depende de su calidad, es decir, entre más precisas y exactas sean las muestras biométricas y las plantillas recolectadas y generadas, será necesario recolectar un menor número de muestras biométricas por individuo.

Recomendaciones relacionadas con el deber de confidencialidad:[24] No difundir datos biométricos a terceros sin consentimiento de su

[21] *Ibidem*, p. 29.

[22] *Ibidem*, p. 31.

[23] *Ibidem*, p. 32.

[24] *Ibidem*, p. 42.

titular; mantener el secreto de la información relacionada con los datos biométricos recabados y almacenados, excepto cuando su comunicación se encuentre permitida en términos de una disposición legal; definir claramente al personal autorizado para tener acceso y para tratar datos biométricos al interior de la organización, e implementarlas medidas de seguridad necesarias para garantizarla secrecía de los datos biométricos.

Recomendaciones relacionadas con el principio de calidad:[25] Los responsables deberán tomar todas las medidas razonables para garantizar que los datos biométricos en su poder sean exactos, completos, pertinentes y actualizados; no conservar los datos biométricos por un plazo superior al necesario para cumplir con la finalidad para la que se han recolectado.

Recomendaciones relacionadas con el régimen de transferencias:[26]Identificar las transferencias que se vayan a realizar de datos biométricos, a fin de cumplir en todos los casos con las obligaciones antes descritas; informar a través del aviso de privacidad las transferencias que se realizarán, el tercero receptor y las finalidades; no realizar transferencias de datos biométricos a terceros no autorizados por los titulares, salvo que se actualicen las excepciones previstas en el artículo 37 de la LFPDPPP o los artículos 22 y 70 de la LGPDPPSO; solicitar el consentimiento expreso y por escrito para transferir datos biométricos, cuándo éstos sean considerados como sensibles; eliminar vínculos innecesarios entre la base de datos biométricos con otros sistemas informáticos o bases de datos que inadvertidamente puedan dar lugar a una transferencia no autorizada, y cifrar los datos biométricos que se transfieran.

Aunado a lo anterior, el INAI precisa que los responsables del tratamiento de datos biométricos, deberán establecer procedimientos o protocolos de actuación para determinar cómo se deberán atender las solicitudes del ejercicio de los derechos al acceso, rectificación, cancelación, oposición y, en su caso, de revocación del consentimiento, así como de la portabilidad, cuando el tratamiento

---

[25] *Ibidem*, p. 34.

[26] *Ibidem*, p. 24.

de datos biométricos se realice por parte de terceros, considerando que quien está obligado a dar atención a las solicitudes es el responsable del tratamiento.[27]

Finalmente, señala que el responsable de tratar datos biométricos, deberá evaluar impacto en la protección[28] de dichos datos personales considerando:

- Si los datos biométricos resultan necesarios y efectivos para atender una necesidad en específico de la organización;
- La comparación del beneficio obtenido por el uso de los datos biométricos versus el costo por una posible violación de la LGPDPPSO, y
- La existencia de una forma menos invasiva para lograr el fin que se persigue.

V. Tratamiento de datos biométricos: seguridad financiera vs protección de datos personales

Con la política de autenticación y verificación biométrica y la creación de la plataforma única de datos biométricos que pretende implementar el gobierno mexicano, se avanza hacia una promesa incumplida de un débil y severamente criticado *Pacto por México*, y es que habrá que recordar que en el año 2012, el presidente de México, Enrique Peña Nieto y los dirigentes de las fuerzas políticas principales del país, firmaron un Acuerdo político que con el objetivo de respetar y defender el derecho a la identidad ciudadana, establece entre otros compromisos, la creación de una cédula única de identificación.[29]

---

[27] *Ibidem*, p. 58.

[28] *Ibidem*, p. 60.

[29] Guerrero Aguirre, Francisco Javier y Amador Hernández, Juan Carlos, *La concertación política en contextos de democracias fragmentadas: el caso PACTO POR MÉXI-*

El pretendido interés de la llamada cédula de identidad ciudadana, guarda estrecha relación con la plataforma única de datos biométricos, ya que como se ha dicho en líneas anteriores, esta plataforma se vinculará directamente con información de Dependencias y Entidades del Gobierno Federal, a fin de integrar un registro único que autentique y verifique la identidad de los ciudadanos mexicanos. Desde mi punto de vista, a partir de estas políticas, los mexicanos eventualmente, contaremos con una sola credencial que permitirá identificarnos en registros migratorios, de seguridad social, laborales, bancarios, policiales, etc., cuyo beneficio principal impactará en la reducción de riesgos de suplantación de identidad.

Pese a que en una primera aproximación, la recolección y el uso de datos biométricos se presentan como propuestas innovadoras del joven siglo XXI, dichos controles pueden tener repercusiones mucho más trascedentes que la simple creación de un registro de identificación o de una política de combate al robo de identidad; con base en los resultados de esta investigación, nace una genuina preocupación en relación con el derecho fundamental a la protección de datos personales ante los efectos que pueda tener el tratamiento para la vida cotidiana.

Hablando de seguridad, al rededor del mundo los ciberataques han puesto en tela de juicio la eficacia de los sistemas de identificación biométrica. En lo relativo a las huellas digitales, en el año 2014, un miembro de la red de piratas informáticos *Chaos Computers Club* – la mayor asociación europea de hackers - confesó haber reproducido, a través de un *software* común y ordinario, la huella dactilar de la Ministro de Defensa alemana Ursula Von Der Leyen, a partir de una serie de fotografías e imágenes publicadas en medios de comunicación oficiales.[30]

CO, Ciudad de México, Colección Nuestro Tiempo, 2016, p. 183.

[30] *Red de hackers afirma que clonó huella dactilar de ministra alemana*, BBC News, 29 de diciembre de 2014. Disponible en: <https://www.bbc.com/mundo/ulti-

En esta misma línea de análisis, en el año 2015 el *departamento de defensa y la oficina de manejo de personal* en Estados Unidos, sufrió un ciberataque que permitió a los *hackers*, obtener entre otros datos personales, las huellas digitales de 5.6 millones de empleados gubernamentales.[31] Se sigue de lo anterior, que cualquier dato biométrico que se encuentre almacenado en una base centralizada, puede ser susceptible de apropiación.

Por otra parte, investigaciones realizadas por la Universidad de Alabama en procesos de activación por reconocimiento de voz, demostraron que ese control puede ser superado e incluso, el dato biométrico puede servir como herramienta para generar información falsa; teniendo grabaciones cortas de una persona hablando y con la ayuda de un sintetizador, los investigadores de esta Universidad lograron convertir la voz de un atacante en la de una víctima.[32]

Adicionalmente, es pertinente señalar que los avances de la inteligencia artificial, mediante algoritmos que aprenden a reconocer patrones del habla de una persona y el uso de redes neuronales que imitan las del cerebro humano, ha permitido reproducir la voz de una persona; aunque en la actualidad nos encontramos con modelos incipientes, no podremos negar que los avances en la tecnología, en un futuro no muy lejano, generarán problemas de seguridad.

No obstante lo anterior, en México, el Grupo Financiero Santander al implementar un procedimiento de firma vocal, figuró como la primera Institución en utilizar este dato biométrico; por medio de la frase *"En Banco Santander mi voz es mi firma"*, se realiza un proce-

mas_noticias/2014/12/141229_ultnot_hackeo_huella_dactilar_ministra_alemana_men> (Fecha de consulta: 25/06/2018).

[31] Matassi, Joshua, "Hackers roban 5.6 millones de huellas digitales al gobierno de Estados Unidos" en *FayerWayer*, 24 de septiembre de 2015. Disponible en: <https://www.fayerwayer.com/2015/09/hackers-roban-5-6-millones-de-huellas-digitales-al-gobierno-de-estados-unidos/> (Fecha de consulta: 12/06/2018).

[32] Bejarano, Pablo, "La huella dactilar, la voz, el iris... también se suplantan" en *El Español*, 27 de octubre 2015. Disponible en: <https://www.elespanol.com/ciencia/tecnologia/20151026/74492595_0.html> (Fecha de consulta: 25/06/2018).

dimiento de verificación para acceder a la banca telefónica.[33] Para Ignacio Zorrilla, Director Ejecutivo de Canales de Autogestión en Banco Santander México, la aplicación de voz se configura como una herramienta con un nivel elevado de seguridad, ya que "crea una huella a partir de 16 patrones que se identifican en la voz, como el tono, la velocidad y el timbre".[34]

Ante esta coyuntura, el *hacker* Jan Krissler quien es también investigador de la Universidad Técnica de Berlín, afirmó confiar mucho más en las contraseñas tradicionales que en las huellas dactilares. Asimismo, señaló que los sistemas biométricos que han sustituido las contraseñas mediante escaneos faciales, de iris o huellas, pueden ser esquivados fácilmente; explicó que el *software* de reconocimiento facial puede ser engañado por la fotografía de cualquier persona, en tanto que impresiones falsas pueden engañar a un sensor de huellas dactilares.[35]

Así, frente a la política de combate a la suplantación de identidad que la CNBV ha implementado a partir del año 2017, interesa reparar en los protocolos de seguridad implantados por las instituciones bancarias. En el punto de partida de esta secuencia y ante la diseminación del uso de ficheros de almacenamiento de datos personales, baste señalar que en los últimos cuatro años, los Bancos

---

[33] De acuerdo con el Director Ejecutivo de Canales de Autogestión del Banco Santander, Ignacio Zorrilla *"cada vez que una persona llama a banca en línea y registra su voz, la información va directamente a los servidores de Santander en Querétaro, donde se almacena la huella de todos los clientes";* como podrá advertirse, la Institución Financiera almacena datos biométricos, para realizar protocolos de autenticación. *Vid. Santander usa 'firma de voz' en banca telefónica*, Excélsior, 09 Diciembre 2013. Disponible en: <http://diario.mx/Economia/2013-12-09_2d072bf9/santander-usa-firma-de-voz-en-banca-telefonica/> (Fecha de consulta: 29/07/2018).

[34] *Idem.*

[35] Ollero, Daniel, "Un hacker reproduce la huella de la ministra de defensa de Alemania" en *El Mundo*, 30 de diciembre de 2014. Disponible en: <http://www.elmundo.es/economia/2014/12/30/54a19eea268e3ec7718b4592.html> (Fecha de consulta: 15/06/2018).

con más presencia en nuestro país, han sido multados en su conjunto por más de trescientos millones de pesos, por el uso inadecuado de datos personales.

En este contexto, Francisco Javier Acuña, Consejero Presidente del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales señaló meses atrás que "hay un extendido mercado negro de las bases de datos personales que instituciones bancarias, empresas telefónicas, tiendas departamentales, agencias de viajes, de venta de tiempos compartidos, entre otras, tienen en su poder y utilizan ilegalmente el listado adquirido".[36]

A la luz de todo lo dicho, el tratamiento de cualquier dato de identificación biométrica como mecanismo de identificación y verificación, tiene graves implicaciones en el ámbito social y jurídico; en relación con el primero, la facilidad con la que dichos datos pueden recrearse, representa un riesgo para la seguridad de los individuos, así como una invasión a su esfera más íntima.

En lo que respecta al campo jurídico, con base en lo que se expone en las siguientes líneas, se puede afirmar que las disposiciones que prevén el almacenamiento masivo de datos biométricos, al no cumplir con los principios de proporcionalidad y legalidad, vulnera el derecho fundamental a la protección de datos personales.

1. Violación al Principio de proporcionalidad:

Como es sabido, el derecho a la protección de los datos personales se regula a través de ocho principios, los cuales se traducen en obligaciones concretas para los responsables en el tratamiento; a saber:

---

[36] Franco, Luciano, "Hay un extendido mercado negro de datos personales: Francisco Javier Acuña" en *Crónica*, 12 de septiembre de 2017. Disponible en: <http://www.cronica.com.mx/notas/2017/1042949.html> (Fecha de consulta: 20/06/2018).

licitud, lealtad, consentimiento, información, proporcionalidad, finalidad, calidad y responsabilidad.[37]

En lo concerniente al principio de proporcionalidad, el artículo 45 del Reglamento de la ley de la materia establece que "sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido".[38] Este principio implica la obligación de evaluar si las finalidades con las que son tratados los datos personales pueden perseguirse de manera menos intrusiva.

Sobre el tema que nos ocupa, de conformidad con lo señalado en el artículo 51 Bis 2 y el Anexo 71 de las DCGIC, cuando las Instituciones opten por la conformación de una base de datos de huellas dactilares, el primer proceso "deberá consistir en capturar en primer lugar las diez huellas dactilares de los empleados, directivos y funcionarios de las Instituciones que estarán a cargo de capturar las huellas de los clientes y posteriormente las correspondientes a estos".[39]

Por su parte, el Acuerdo del Consejo General del Instituto Nacional Electoral, por el que se aprueba la implementación del servicio de verificación de los datos de la credencial para votar, que servirá para garantizar el derecho de protección de datos de los ciudadanos, contenidos en el padrón electoral y que tiene como objetivo "autenticar las huellas dactilares del ciudadano que se identifiquen con una Credencial para Votar, mediante la correlación gráfica de las marcas dactilares capturadas al momento de presentar dicho instrumento electoral, con aquellas que se encuentran almacenadas

---

[37] Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante, LFPDPPP), DOF, 05/07/2010. *Vid.* Artículo 6.

[38] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, DOF, 21/12/2011.

[39] Resolución que modifica las Disposiciones de Carácter General aplicables a las Instituciones de Crédito, *Op. Cit.*, nota 6. *Vid.* Artículo 51 Bis 2 y Anexo 71.

en la base de datos del Padrón Electoral",[40] establece con relación al principio de proporcionalidad, que el *servicio de verificación* de los datos de la *credencial para votar* considera únicamente como datos necesarios para su ejecución: el nombre, apellido paterno, apellido materno y la clave de elector del ciudadano, y de ser necesario, las huellas dactilares del dedo índice de ambas manos. Como se puede advertir, para el INE, las huellas dactilares de los dos dedos índices, son suficientes para realizar el procedimiento de autenticación.

En esta línea de razonamiento, las disposiciones establecidas en las DCGIC que prevén la captura de las diez huellas dactilares, son violatorias del principio de proporcionalidad, ya que el procedimiento de verificación ante el INE, solo se realizará a través de las huellas digitales de los dedos índices, siendo innecesaria la captura indiscriminada de las crestas papilares de los diez dedos de la mano.

Nótese entonces que del mismo modo, la plataforma única de datos biométricos que prevé implementar el gobierno mexicano, se traduce en un excesivo uso de técnicas de identificación, considerando que puede realizarse un procedimiento de autenticación sin la necesidad de memorizar los datos biométricos en una base centralizada. En su caso, resulta preferible, a efecto de reducir los riesgos, almacenar la biometría en un objeto disponible exclusivamente para el usuario (como una tarjeta con microchip, un teléfono móvil o una tarjeta bancaria). A manera de ejemplo, la autoridad alemana de protección de datos aprobó el uso de datos biométricos en los documentos de identidad con objeto de evitar su falsificación, siempre que los datos se almacenen en el microchip de la tarjeta y

---

[40] Acuerdo del Consejo General del Instituto Nacional Electoral, por el que se aprueba la implementación del Servicio de Verificación de los datos de la Credencial para Votar, que servirá para garantizar el derecho de protección de datos de los ciudadanos, contenidos en el Padrón Electoral, DOF, 12/04/2016.

no en una base de datos para compararlos con las huellas digitales del propietario.[41]

Por lo anterior, se arguye que cualquier base centralizada de almacenamiento de datos biométricos, resulta desproporcional a la luz de los principios fundamentales de protección a la información personal.

2. Principio de Legalidad

El principio de legalidad se traduce en que los datos personales deberán recabarse y tratarse de manera lícita y su obtención no deberá hacerse a través de medios engañosos o fraudulentos.[42]

De ello, se interpreta que para que las instituciones financieras realicen un tratamiento de datos biométricos en plena observancia al principio de legalidad, deberán precisar en sus respectivos avisos de privacidad, que dentro de los datos sensibles a tratar se encuentran datos de identificación biométrica, al tiempo de señalar, la finalidad de dicho tratamiento. En el caso particular de las huellas dactilares, se deberá establecer el número de huellas dactilares a recabar.

Así, del análisis realizado a diversos avisos de privacidad, se concluye que las instituciones financieras vulneran notoriamente el principio de legalidad al que se hace referencia en este epígrafe. Por ejemplo, el aviso de privacidad del Grupo Financiero Santander México[43] señala en su numeral 3, que recabará diversas categorías de datos personales, entre los cuales se encuentran datos biomé-

---

[41] San Epifanio, Leire Escajedo, *Reconocimiento e identificación de las personas mediante biometrías estáticas y dinámicas*, Alicante, Universidad de Alicante, 2015, p.208.

[42] LFPDPPP, *Op. Cit.,* nota 36. *Vid.* Artículo 7.

[43] Grupo Financiero Santander, Aviso de Privacidad. Disponible en: <https://www.santander.com.mx/PDF/personas/AvisoPrivacidad.pdf> (Fecha de consulta: 24/07/2018).

tricos, sin embargo, no se especifica los tipos a tratar, es decir, no detalla si se refiere a huellas dactilares, rostro, iris o voz.

Adicionalmente, los datos biométricos no se encuentran considerados dentro del inciso (X) en el que se señalan los datos sensibles a tratar; al no considerarse de esta naturaleza, la Institución Financiera conforme a lo estipulado en su Aviso, podrá transferir los datos biométricos a sociedades subsidiarias y podrán tratarlos para finalidades secundarias. Ello, al no privilegiar la expectativa razonable de privacidad y en el entendido que los datos personales proporcionados solo podrán ser tratados conforme a lo acordado entre las partes, viola el principio de legalidad.

Asimismo, la Institución Financiera es omisa en señalar que realizará transferencia de datos con el Instituto Nacional Electoral (INE) con la finalidad de validar la identidad en términos de lo establecido en las DCGIC. En esta tesitura, el Banco Santander, no solo viola el principio legalidad, sino también el de finalidad. Recordemos que conforme a lo establecido en el artículo 12 de la LFPDPPP "El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad".[44] Principio sustentado en la concepción de que todo tratamiento de datos personales se caracteriza por la confianza que deposita cualquier persona en otra para el uso de sus datos personales.

Finalmente, el aviso de privacidad presenta una notable deficiencia cuando establecer que "los Datos Personales Sensibles recabados, se tratarán con la finalidad exclusiva de realizar y dar seguimiento al proceso de contratación de productos financieros catalogados como Seguros que se comercializan por la empresa Zurich Santander Seguros México, S.A.".[45]

De esta manera, se advierte que en el aviso de privacidad no se informa la finalidad específica del tratamiento de datos biomé-

---

[44] LFPDPPP, Op. Cit., nota 36. Vid. Artículo 12.

[45] Grupo Financiero Santander, Aviso de Privacidad. *Op. Cit.,* nota 42.

tricos, siendo que éstos se recaban exclusivamente por el Banco para corroborar la identidad del cliente o usuario. En consecuencia nos enfrentamos a un inminente riesgo de reutilización de datos biométricos.

Por lo que respecta a los avisos de privacidad del Grupo Financiero BBVA Bancomer[46] y Banorte,[47] pese a que ambas Instituciones reconocen el tratamiento de datos biométricos en su calidad de datos sensibles, el primero no prevé específicamente el tratamiento de huellas dactilares, en tanto que el segundo no señala el número huellas dactilares a tratar.

Finalmente, ninguno de los avisos de privacidad analizados en los párrafos anteriores, cumplen con la recomendación del INAI relativa especificar que el tratamiento de datos biométricos se llevará a cabo en dos etapas. La primera, que consiste en la creación de bases de información en las que serán almacenadas los datos de información biométrica y la segunda, para la comparación de nuevas muestras biométricas con las almacenadas previamente.[48]

VI. Conclusiones

En aras de proteger tanto al sector financiero como a los clientes y usuarios de la banca del riesgo que ha representado en los últimos años el robo o suplantación de identidad, en México se ha avanzado hacia la implementación de políticas de autenticación y verificación de identidad a través del procesamiento técnico de datos biométricos. Con la importante precisión que la información biométrica

---

[46] Grupo Financiero BBVA Bancomer, Aviso de Privacidad. Disponible en: <https://www.bancomer.com/personas/aviso-de-privacidad.html> (Fecha de consulta: 18/07/2018).

[47] Grupo Financiero Banorte, Aviso de Privacidad. Disponible en: <https://www.banorte.com/cms/peper/docs/AvisoPrivacidad.html> (Fecha de consulta: 18/07/2018).

[48] INAI, *Op. Cit.*, nota 2, p. 26.

identifica inequívocamente a una persona, resulta necesario que el marco normativo mexicano prevea mecanismos jurídicos adecuados que garanticen un correcto tratamiento de datos biométricos recolectados.

Pese que en nuestro país existen dos legislaciones en materia de protección de datos personales – una aplicable al sector público y otra al sector privado – ninguna de éstas incluyen los datos biométricos; en su caso, conforme a la interpretación del INAI, éstos se consideran dentro de la categoría de datos sensibles. A juicio de la autora, resulta de suma importancia que los cuerpos normativos en materia de protección de datos personales amplíen el concepto de datos sensibles, a fin de reconocer expresamente a los datos biométricos. Con ello, se pretende evitar interpretación subjetiva o controversia respecto al tratamiento del dato biométrico en calidad de dato personal o dato personal sensible.

Por lo que refiere a la plataforma única de datos biométricos que pretenden utilizar las entidades crediticias a partir del año 2019, con base en lo expuesto, se puede afirmar que dicho mecanismo como herramienta de verificación resulta desproporcional e innecesario toda vez que supone utilización de excesivas técnicas de identificación; para realizar el procedimiento de autenticación, es suficiente almacenar los datos personales de manera descentralizada. Para ello, se dispone de la base de datos de huellas dactilares que se señala en el artículo 51 Bis 2 de las DCGIC.

Ante esto, se observa que la base de datos de huellas dactilares, aun cuando no almacena de manera centralizada la información, sí incrementa el riesgo del uso indebido de datos biométricos como medio para obtener información que no está relacionada con la finalidad para la cual fueron obtenidos. Dicho de otro modo, el acceso indiscriminado a bases que contengan huellas dactilares, favorecerá el intercambio de información que se encuentre registrada en diversas bases de datos personales, permitiendo por ejemplo, conocer el perfil psicológico y médico de un individuo, su origen

racial y en el caso más extremo, robar su identidad, causando un daño irreparable a los interesados.

Por consiguiente, si se va a utilizar dicha base, se percibe indispensable el establecimiento de estándares de regulación y de protección de datos biométricos. En primer lugar, deberá señalarse en la ley de la materia, así como en los respectivos avisos de privacidad, que los datos biométricos serán tratados estrictamente para el proceso de verificación que señalan las DCGIC; en consecuencia, no podrán utilizarse para realizar un procedimiento de identificación. En segunda instancia, se deberá prever que las Instituciones Financieras, solo podrán transferir datos biométricos con el Instituto Nacional Electoral, o en su caso, precisar las autoridades con las que se va a verificar la coincidencia. Por último, se deberá regular el tratamiento exclusivo de las huellas dactilares de los dedos índices, al tiempo de establecer que las mismas serán destruidas, en el momento en que el usuario deje de tener relación con la entidad financiera.

Concluyendo, como medida de seguridad técnica para una adecuada protección de datos, se sugiere codificar los controles de acceso e implementar claves para la reconstrucción de los datos originales a partir de la información almacenada. Si la descodificación se hiciera a partir de los datos biométricos del propio interesado, se evitaría la creación de bases de datos con información biométrica que pudiera reutilizarse para fines ajenos.

VII. Fuentes de información

1. Bibliografía

Aparicio Salom, Javier, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Navarra, Aranzadi, 2000.

Guerrero Aguirre, Francisco Javier y Amador Hernández, Juan Carlos, *La concertación política en contextos de democracias fragmentadas: el caso PACTO POR MÉXICO*, Ciudad de México, Colección Nuestro Tiempo, 2016.

SAN EPIFANIO, Leire Escajedo, *Reconocimiento e identificación de las personas mediante biometrías estáticas y dinámicas*, Alicante, Universidad de Alicante, 2015.

2. HEMEROGRAFÍA

NEIRA ORJUELA, Fernando, "Biometría y control migratorio en América Latina" en *Cuadernos de H Ideas*, Argentina, Vol. 9, Núm. 9, diciembre 2015, pp. 2-5.

3. MESOGRAFÍA

BEJARANO, Pablo, "La huella dactilar, la voz, el iris... también se suplantan" en *El Español*, 27 de octubre 2015. Disponible en: <https://www.elespanol.com/ciencia/tecnologia/20151026/74492595_0.html> (Fecha de consulta: 25/06/2018).

FRANCO, Luciano, "Hay un extendido mercado negro de datos personales: Francisco Javier Acuña" en *Crónica*, 12 de septiembre de 2017. Disponible en: <http://www.cronica.com.mx/notas/2017/1042949.html> (Fecha de consulta: 20/06/2018).

Grupo Financiero Santander, Aviso de Privacidad. Disponible en: <https://www.santander.com.mx/PDF/personas/AvisoPrivacidad.pdf> (Fecha de consulta: 24/07/2018).

Grupo Financiero BBVA Bancomer, Aviso de Privacidad. Disponible en: <https://www.bancomer.com/personas/aviso-de-privacidad.html> (Fecha de consulta: 18/07/2018).

Grupo Financiero Banorte, Aviso de Privacidad. Disponible en: <https://www.banorte.com/cms/peper/docs/AvisoPrivacidad.html> (Fecha de consulta: 18/07/2018).

Grupo "Protección de Datos" del Artículo 29, WP 248 rev.01: Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, Bruselas, 2017. Disponible en: <https://www.aepd.es/media/criterios/wp248rev01-es.pdf> (Fecha de consulta: 18/09/2018).

Guía para el tratamiento de Datos Biométricos, Ciudad de México, INAI, 2018. Disponible en: <*h*ttp://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf> (Fecha de consulta: 15/09/2018).

Scheinin, Martin, Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, 2009. Disponible en: <http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> (Fecha de consulta: 18/09/2018).

Juárez, Edgar, "CNBV arrancará supervisión en línea del sector financiero" en *El Economista*, 19 de junio de 2015. Disponible en: <https://www.eleconomista.com.mx/sectorfinanciero/CNBV-arrancara-supervision-en-linea-del-sector-financiero-20180619-0154.html> (Fecha de consulta: 22/06/2018).

Matassi, Joshua, "Hackers roban 5.6 millones de huellas digitales al gobierno de Estados Unidos" en *FayerWayer*, 24 de septiembre de 2015. Disponible en: <https://www.fayerwayer.com/2015/09/hackers-roban-5-6-millones-de-huellas-digitales-al-gobierno-de-estados-unidos/> (Fecha de consulta: 12/06/2018).

Ollero, Daniel, "Un hacker reproduce la huella de la ministra de defensa de Alemania" en *El Mundo*, 30 de diciembre de 2014. Disponible en: <http://www.elmundo.es/economia/2014/12/30/54a19eea268e3ec7718b4592.html> (Fecha de consulta: 15/06/2018).

Red de hackers afirma que clonó huella dactilar de ministra alemana, en *BBC News*, 29 de diciembre de 2014. Disponible en: <https://www.bbc.com/mundo/ultimas_noticias/2014/12/141229_ultnot_hackeo_huella_dactilar_ministra_alemana_men> (Fecha de consulta: 25/06/2018).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>, (Fecha de consulta: 28/06/2018).

Resolución que modifica las disposiciones de carácter general aplicables a las instituciones de crédito, DOF, 29/08/2017. Disponible en: <https://www.cnbv.gob.mx/Resoluciones%20Modificatorias/100a.%20Resoluci%C3%B3n%20modificatoria%20CUB.pdf> (Fecha de consulta: 22/05/2018).

Santander usa 'firma de voz' en banca telefónica, en *Excélsior*, 09 Diciembre 2013. Disponible en: <http://diario.mx/Economia/2013-12-09_2d072bf9/santander-usa-firma-de-voz-en-banca-telefonica/> (Fecha de consulta:29/07/2018).

4) Legisgrafía

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, DOF, 05/07/2010. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, DOF, 21/12/2011. Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf>.

Acuerdo del Consejo General del Instituto Nacional Electoral, por el que se aprueba la implementación del Servicio de Verificación de los datos de la Credencial para Votar, que servirá para garantizar el derecho de protección de datos de los ciudadanos, contenidos en el Padrón Electoral, DOF, 12/04/2016. Disponible en: <http://www.dof.gob.mx/nota_detalle.php?codigo=5432730&fecha=12/04/2016>.