Universidad de Buenos Aires

Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Protección de datos biométricos en Argentina:

Análisis del marco legal vigente y de las tecnologías incorporadas a su almacenamiento.

Autora: Lic. Virginia Isabel Mayer

Directora de la Tesis: Mg. Patricia Prandini

Año de Presentación: 2020

Cohorte de la Maestranda: 2017

Por medio de la presente, la autora manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual

FIRMADO
Virginia Isabel MAYER
DNI 14.087.990

RESUMEN

La biometría y en particular el uso de huellas dactilares es uno de los métodos más tradicionales y efectivos. Por esta razón, su utilización se ha expandido a ritmo creciente durante los últimos años al permitir mecanismos de autenticación o verificaciones masivas de identidad en escasos segundos, en un lugar dado y con un grado suficiente de confiabilidad.

Al mismo tiempo, han crecido los riesgos en relación con la protección de los datos personales implicados en los biométricos. El uso de las tecnologías asociadas presenta un grave desafío al derecho de las personas a que sus datos personales sean adecuadamente protegidos. Los datos biométricos brindan información sobre la intimidad del cuerpo humano. A su vez, el carácter permanente de ellos impide que en caso de ser divulgados de manera ilegítima, el daño pueda ser reparado, toda vez que, a diferencia de una contraseña, no es posible volver a configurar nuestra huella digital o la imagen de nuestro rostro.

El presente trabajo pretende indagar en la madurez del marco normativo argentino para la protección de datos personales de carácter biométrico, sobre todo durante el almacenamiento de los mismos, así como en las tecnologías disponibles y utilizadas para tal propósito.

Asimismo, se plantea la hipótesis de que existen tecnologías recientes que podrían adecuarse al efecto de un mejor control de los riesgos que afectan al almacenamiento de los datos biométricos, contribuyendo por ello al fortalecimiento del marco normativo.

La metodología de este trabajo incluye, entre otras actividades que se apreciarán a lo largo de su desarrollo, la revisión de normas emanadas a partir de la Ley de Protección de Datos Personales, la indagación bibliográfica respecto de las tecnologías relativas a la biometría y la revisión de la experiencia dada por el sistema de ANSES “Mi Huella”.

Palabras clave

Datos personales | Biometría | Riesgos | Tecnologías de almacenamiento | SBA o Mi Huella | Normas argentinas de protección de datos personales | Anonimización.

Tabla de contenido

Tabla de Tablas e Ilustraciones

Capítulo I - INTRODUCCIÓN

1.1. Antecedentes generales

La biometría es un método tradicional de identificación de las personas: las huellas dactilares, el ejemplo más clásico, se usan desde hace décadas. Sin embargo, en los últimos tiempos algunas circunstancias han acelerado el interés en estas técnicas. En primer término, existe una necesidad creciente de identificación inequívoca de personas en todos los ámbitos, público o privados, provocada tanto por amenazas a escala mundial, cuanto por el incremento del delito basado en la usurpación de identidad en general para la malversación de fondos. En segundo lugar, las nuevas tecnologías basadas en biometría parecen dar respuesta efectiva a esos problemas al ofrecer mecanismos de autenticación o verificaciones masivas de identidad en escasos segundos, en un lugar dado y con un grado suficiente de confiabilidad.

Desde el punto de vista del marco normativo aplicable en Argentina, el principal antecedente a considerar es la Ley N° 25.326 de Protección de Datos Personales y sus modificaciones y reglamentaciones que han establecido en el orden jurídico de la Argentina las bases conceptuales al señalar como objeto de la referida ley la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional [1]. Asimismo, esta legislación local ha ido evolucionando y en general, perfeccionándose, al compás de impulsos similares en otras legislaciones de referencia regional u occidental (principalmente la Unión Europea y USA).

A partir de la mirada normativa, surge de inmediato el punto de vista institucional, es decir el de las organizaciones que reciben los mandatos, facultades y expresiones de competencias determinadas por las normas. En

[1] Artículo 1° de la Ley N° 25.326 Referencia bibliográfica [1]

Argentina la Agencia de Acceso a la Información Pública (AAIP)[2] es, a partir del 17 de septiembre de 2017, la autoridad de aplicación de la Ley de Protección de Datos Personales. Esta competencia era detentada hasta ese momento por la Dirección Nacional de Protección de Datos Personales (DNPDP), que fuera creada en la órbita de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos, por medio del Decreto N° 1558 del 29 de noviembre de 2001, reglamentario de la Ley de Protección de Datos Personales.

De esta manera, el registro de las bases de datos personales que era competencia de la Dirección Nacional de Protección de Datos Personales, al integrarse este organismo a la estructura de la Agencia de Acceso a la Información Pública, naturalmente queda en la órbita de quien es la nueva autoridad de aplicación de la Ley de Protección de Datos Personales.

Es decir que el organismo que actúa como autoridad de aplicación de la ley de acceso a la información pública también lo es de la ley de protección de datos personales. Se podría reflexionar prima facie que el legislador ha pretendido asegurar el acceso público y promover la transparencia sobre la información que pueda ser pública, definiendo el carácter de público como aquello que no debe estar protegido.

Desde la perspectiva de las técnicas y más aún desde las tecnologías, el cúmulo de antecedentes a considerar luce mucho más voluminoso y de alguna manera se presenta en cada caso como precedente a lo legislativo. Primero, el hallazgo tecnológico y posiblemente luego, el ordenamiento jurídico al respecto. A partir de dicha premisa, es muy probable que se pueda constatar una brecha importante entre las normas y reglamentos vigentes y las tecnologías disponibles para el almacenamiento y la protección de los datos personales.

Cabe destacar que no resulta sencillo disociar los conceptos ni los mecanismos de almacenamiento con los de protección de datos. El almacenamiento, guarda o registro de los datos personales se practica para que estén disponibles e íntegros cuando se requieran y eso mismo implica cuidarlos y protegerlos de los riesgos que los asechan (riesgos de pérdida de integridad,

[2] Fue creada en el ámbito de la Jefatura de Gabinete de Ministros por la Ley N° 27.275 de Derecho de Acceso a la Información Pública. Referencia Bibliográfica [2].

destrucción, sustracción, adulteración, imposibilidad de acceso, acceso indebido por quien no está autorizado, etc.). Por otro lado, los cuidados y los mecanismos de protección se dan sobre un medio o un soporte de almacenamiento determinado, no en el vacío. Es decir que analizar el tipo o las características que debería tener o tiene un cierto esquema de almacenamiento, implica avanzar sobre dichas características, los modelos y los métodos o procedimientos de protección de los datos que almacene.

En cuanto a cuáles tecnologías deberían considerarse para el análisis relacionado con los mecanismos de almacenamiento y protección, se advierte que deberían tomarse en cuenta todas las directamente relacionadas y algunas que seguramente inciden de manera indirecta. Entre las primeras incluimos técnicas criptográficas y sus implementaciones habituales, técnicas de organización, búsqueda y recupero de lo almacenado (motores de bases de datos) y medios de almacenamiento (por ejemplo, nube en sus variantes pública, privada e híbrida) entre las más importantes. Las indirectas refieren a las técnicas y algoritmos de representación digital de los datos biométricos en sí.

1.2. Situación actual en Argentina

En al apartado anterior se mencionó el pilar fundamental de la legislación en la Argentina sobre el almacenamiento y la protección de datos personales. Ahora se dirá, como una de las hipótesis del presente trabajo, que esa legislación va en líneas generales demorada y por detrás del veloz avance de las tecnologías. No obstante, podemos ver que algunos instrumentos han ido evolucionando de alguna manera, tratando de adaptarse aunque sea de una forma parcial o insuficiente. Por caso, el relativo a la transformación de la autoridad de aplicación de la legislación de base que acaba de señalarse.

Por otra parte, la facilidad e inmediatez de los actuales mecanismos de captura de huellas dactilares, así como el creciente abaratamiento de sus costos, ha redundado en sistemas cada vez más disponibles, cercanos y atractivos para un uso inmediato y muy variado en cuanto a su finalidad, aun cuando en general refiere a la identificación o confirmación de identidad de personas. Es posible entonces señalar un enorme conjunto de tecnologías asequibles en relación con

sistemas de captura y almacenamiento de datos biométricos, sobre todo para los más usuales que son los de huellas dactilares y los de reconocimiento facial.

Asimismo es relevante considerar el grado de madurez de las diferentes soluciones tecnológicas en cuanto a los riesgos fundamentales de la seguridad informática, es decir los relativos a la confidencialidad, la integridad y la disponibilidad de los datos biométricos. Ello sin dejar de señalar que los criterios de evaluación de dichos riesgos quizás tampoco hayan alcanzado una madurez suficiente, o presenten serias dificultades al combinarse con los propios de otras tecnologías (por ejemplo, los de computación en la nube).

Lo cierto es que hay cuestiones de gran riesgo y de alto impacto asociadas al almacenamiento biométrico, por el simple motivo que se trata de datos personales, únicos e irrepetibles para su titular, es decir la persona humana a quien pertenecen. Pongamos por caso que una base de datos de huellas dactilares, una de las más clásicas técnicas de biometría, fuera atacada ("*hackeada*"). Es decir, accedida sin autorización, hurtada, divulgada a terceros, malversada o utilizada con fines maliciosos de cualquier tipo: ¿qué daños sufrirían los usuarios involucrados en dicha base? Para un usuario es posible, con menor o mayor dificultad, cambiar una contraseña tradicional (frase, secuencia de caracteres alfanuméricos, etc.), pero es imposible cambiar su huella digital, lo que implica que quizás nunca más pueda volver a utilizarla como identificador biométrico.[3]

Otro aspecto de relevancia a tener en cuenta es el impulso que el sector público, en particular la administración pública nacional (AFIP, ANSES y la mayoría de las reparticiones gubernamentales del nivel nacional o federal) han dado al registro de datos biométricos. Por ejemplo, el sistema Mi Huella de ANSES, el cual se presenta como un sistema que permite reconocer la identidad de las personas a través de la digitalización de las huellas dactilares con el objeto de facilitar la realización de trámites, con un despliegue de grandes proporciones, dado que el sistema de reconocimiento tiene que estar disponible en

[3] Ref. Bibliográfica [3] David Sarmiento - TOC: ¡No al almacenamiento de datos biométricos en la nube! - 23 enero 2015 - http://www.chw.net/2015/01/toc-no-al-almacenamiento-de-datos-biometricos-en-la-nube/

prácticamente la totalidad de los cajeros automáticos del país, además de considerar el enrolamiento de las huellas dactilares en cada uno de los puntos de atención del sistema bancario dispuestos para ello y, por fin, en alguna etapa ulterior, liberar el mecanismo y sus procedimientos para volverlos masivamente disponibles para todos los usuarios de la banca personal.

Para terminar, otro aspecto de la tecnología actual que resulta insoslayable, es el uso cada vez más extendido de las aplicaciones móviles. La operatoria bancaria y la mayoría de las aplicaciones gubernamentales o comerciales, comienzan a interesarse en la autenticación por medio del teléfono celular y a través del uso de datos biométricos.

1.3. Definición de la situación problemática

El problema se plantea como un conjunto de interrogantes a resolver:

a. ¿El marco normativo en vigencia es suficiente para el grado de evolución y de divulgación o masividad que han alcanzado las tecnologías sobre biometría en el país?

Dar respuesta a este interrogante implica estudiar la consistencia de la legislación existente sobre la protección de datos personales y en particular sobre el uso o desarrollo de sistemas biométricos y sus medios de almacenamiento. Pero no solo la consistencia, coherencia e integralidad de las normas, reglamentaciones y criterios en uso, sino también la flexibilidad que evidencian a los efectos de contener el devenir de tecnologías de irremediable y muy veloz evolución.

b. Los sistemas de almacenamiento de datos biométricos que se utilizan en Argentina, ¿están suficientemente desarrollados en relación con la comprensión y evaluación de los riesgos que entrañan respecto de la protección ofrecida?

Isai Rojas González y Gabriel Sánchez Pérez [4] señalan los riesgos que podrían presentarse ante un sistema biométrico que no esté adecuadamente protegido. El más inmediato de ellos sería la obtención de información personal sensible, con el agravante de que no sería necesario que dicha información tuviera identificación de tipo alfanumérica. Por ejemplo, la colección de caras de los empleados de una organización, utilizada en un sistema de reconocimiento facial interno, podría dar pie a algún análisis de tipo discriminatorio en relación con la raza o el origen étnico de los mismos.

También señalan otra situación riesgosa de alto impacto dada porque algunos datos biométricos pueden ser obtenidos realizando el proceso inverso al de captura y almacenamiento, como es el caso de las huellas dactilares. Las huellas tienen rasgos únicos conocidos como minucias y son precisamente estas minucias las que son reconocidas durante el proceso de captura, luego codificadas y por fin, almacenadas como una secuencia de datos denominada plantilla de minucias. Estimativamente, una huella dactilar reconstruida a partir de la plantilla de minucias es efectiva en por lo menos el 90% de los casos. Por lo tanto, existe cierta facilidad tecnológica para la manipulación de huellas dactilares reconstruidas desde una base de datos de plantillas de minucias. Además, si bien no es necesario almacenar la imagen fotográfica de una huella dactilar, lo más probable es que la mayoría de los sistemas no prescindan de ellas.

Esto nos lleva a una tercera cuestión que podría ser la conjunción de las dos anteriores.

c. La administración de los riesgos inherentes al uso de los sistemas biométricos y su almacenamiento en particular, ¿está suficientemente comprendida y regulada en el marco normativo de aplicación?

La recolección de datos biométricos es otro aspecto de preocupación y así los señalaron diferentes estudios en el sentido de que todos vamos dejando “rastros de datos biométricos” de manera habitual y prácticamente involuntaria que podrían ser recolectados y utilizados sin nuestro conocimiento. Entonces,

[4] Ref. Bibliográfica [4] Isai Rojas González y Gabriel Sánchez Pérez - 2012 - LEYES DE PROTECCIÓN DE DATOS PERSONALES EN EL MUNDO Y LA PROTECCIÓN DE DATOS BIOMÉTRICOS PARTE 2 Para Revista .Seguridad UNAM Nro. 14 “Gestión de Seguridad y Riesgos” de septiembre de 2012 (https://revista.seguridad.unam.mx/numeros/numero-14)

considerando esta cuestión, es de interés analizar qué recaudos toma la legislación argentina al respecto y si son suficientes en relación con los riesgos que se corren.

Cabe señalar que lo anterior es uno de los tantos aspectos riesgosos derivados de los usos y prácticas actuales en relación con el almacenamiento de datos biométricos. Es dable citar algunos otros habituales o inmediatos, a saber:

- Almacenamiento en la nube mediante instrumentos contractuales débiles, desconocidos o ajenos a la legislación argentina.
- Uso insuficiente o precario de elementos, técnicas o procedimientos de protección de datos en el almacenamiento, tales como enmascaramiento, disociación, ocultamiento, cifrado, separación, agregado y técnicas propias del Big Data tales como anonimización o seudonimización, entre otros.
- Almacenamiento en el dispositivo móvil mediante esquemas inseguros.

En todos los casos interesa analizar tanto la madurez del marco normativo aplicable cuanto la de los desarrollos tecnológicos disponibles.

1.4. Objetivos

1.4.1. General

Evaluar el grado de madurez técnico y legal alcanzado en el plano nacional de la República Argentina respecto de la protección en el almacenamiento de datos biométricos

1.4.2. Específicos o particulares.

Compendiar, analizar y valorar las normas existentes en el plano nacional orientadas a la protección de datos personales y biométricos, en términos de efectividad y cobertura.

Compendiar, analizar y valorar las tecnologías de almacenamiento disponibles, utilizadas o adecuadas a ese fin, desde el punto de vista de la protección que ofrecen ante los riesgos que atentan contra la disponibilidad, la integridad y la confidencialidad de los datos biométricos.

Revisar y valorar el caso de almacenamiento de datos biométricos del sistema de ANSES Mi Huella, desde el punto de vista de cumplimiento normativo y de apropiación o uso de tecnologías efectivas.

1.5. Enfoque metodológico del trabajo

1.5.1. Alcance y limitaciones

El estudio abarcará aspectos técnicos relacionados al marco normativo existente en Argentina para la protección y el almacenamiento de los datos biométricos. Fundamentalmente se compilará, revisará y evaluará en términos de suficiencia y madurez alcanzadas la legislación constituida por las leyes N° 25.326 de Protección de Datos Personales y N° 27.275 de Acceso a la Información Pública, sus respectivos decretos reglamentarios, normas modificatorias en general y proyectos legislativos con estado parlamentario.

En particular se incluirá en el análisis la normativa emanada de la Dirección Nacional de Protección de Datos Personales (DNPDP) y más recientemente de la Agencia de Acceso a la Información Pública (AAIP), ambas en el ámbito de la Jefatura de Gabinete de la Nación, por su carácter sucesivo de autoridades de aplicación de la legislación sustantiva en el tema.

Para la valoración de las normas vigentes respecto de la protección de datos biométricos, especialmente en la faz relativa al almacenamiento, se tomarán criterios basados la validez, el grado de cobertura del fenómeno al que están dirigidas y su eficacia en el sentido de determinar si las normas son cumplidas por las personas a las que se dirigen, es decir sus destinatarios o sujetos de derecho. Además, si en caso de ser violadas dichas normas, existen instrumentos o medios coercitivos por parte de las autoridades que las han impuesto para que se las haga valer.

A fin de darle mayor precisión al alcance de la evaluación del marco normativo dedicado a la protección de datos biométricos dentro de los términos de esta propuesta, se pone de manifiesto que el conjunto de criterios a utilizar, excluye expresamente los que pudieran ser relativos a la justicia o a la moral.

En relación con los aspectos tecnológicos, se efectuará una revisión de las tecnologías en uso para la protección de datos, impulsadas por las normas y reglamentaciones en vigencia o no. En particular, se privilegiará para el análisis los datos biométricos obtenidos a partir de huellas dactilares, entendiendo que es el sistema más extendido en su uso actualmente y el que presenta mayor potencial de despliegue o divulgación. Por lo cual, el trabajo no incluirá aspectos de referencia general o pormenorizada sobre otras técnicas en uso, tal como la de reconocimiento facial.

Respecto de los usuarios de dichas tecnologías, se concentrará el análisis sobre el sistema Mi Huella de ANSES en todos los aspectos relativos al almacenamiento y protección de los datos biométricos, tanto desde el punto de vista tecnológico como de cumplimiento del marco normativo de aplicación.

1.5.2. Cuestiones teóricas o prácticas a aportar al campo temático

La cuestión problemática que se ha venido planteando, para decirlo en pocas palabras, es que deberíamos proteger de la identificación maliciosa o con fines delictivos a datos cuya naturaleza y propósito es precisamente servir a la identificación.

Desde esa perspectiva resulta evidente que no podemos aplicar del mismo modo toda la artillería destinada a la anonimización, seudonimización o disociación, tan efectivas en todo lo relativo a Big Data, porque con ese uso tradicional o extremo anularíamos, o volveríamos demasiado ineficiente, la principal capacidad de los datos biométricos que es la destinada a la identificación de su titular.

Sin embargo, es posible inferir que algunas de las técnicas referidas en los apartados anteriores pueden adaptarse o adecuarse con buenas perspectivas de éxito en la encomienda de proteger a los datos biométricos, especialmente en su almacenamiento.

En particular, las cuestiones de ocultamiento mediante el cifrado y las de separación de los datos en espacios de almacenamiento distintos son de gran interés. Así, uno de los primeros aportes al campo de estudio podría

conceptualizarse como el análisis de cuán adaptables y efectivas serían determinadas técnicas propias del manejo de *Big Data*, para el caso del almacenamiento y protección de datos biométricos.

Otro aporte, más que nada teórico, estaría dado por la revisión exhaustiva y posterior valoración del marco normativo específico existente en el país, aplicable a los medios y métodos de almacenamiento de datos biométricos: regulaciones, prohibiciones o recomendaciones dadas por las normas vigentes en la materia.

Una aproximación preliminar a una contribución específica que se propone en relación con las tecnologías de almacenamiento, refiere a las recomendación de que los vectores de los datos de reconocimiento biométrico sean cifrados mediante alguna función de *hashing* y ésta sea la clave de vinculación entre dichos datos y los datos alfanuméricos respectivos a la identidad de la persona, desde el momento del almacenamiento en sí y luego para cada consulta o recupero de información.

Asimismo, como contribución práctica y concreta, se propone avanzar respecto del proyecto Mi Huella y sus experiencias tanto en lo relativo a las tecnologías de almacenamiento y protección utilizadas, cuanto al grado de cumplimiento de las normas vigentes al respecto y, como contracara, la detección de vacíos legales sobre el tema específico.

1.5.3. Hipótesis del trabajo

Como consecuencia de lo enunciado en el apartado anterior, las principales hipótesis de estudio son:

- El marco normativo existente es insuficiente en cuanto a la cobertura y orientación sobre la protección que ofrece para datos personales en general y biométricos en particular.
- En virtud de esa insuficiencia, de cierto retraso respecto de la evolución de determinadas tecnologías tales como big data, nube o biometría, además del uso creciente alcanzado por las mismas, podría tipificarse ese marco como poco robusto o directamente inmaduro.

- Existen oportunidades de mejora en relación con las tecnologías en uso para el almacenamiento de datos biométricos y el grado de protección que estas ofrecen para esos datos, tomando en cuenta los principales riesgos a los que están expuestos.
- A su vez, la comprensión de esas mejoras tecnológicas podrían impactar en el marco normativo que se supone débil y contribuir a su fortalecimiento.

1.5.4. Estructura del trabajo

Es posible señalar tres componentes fundamentales en el desarrollo del presente trabajo:

- El estudio del marco normativo de alcance nacional dedicado a la protección en el almacenamiento de los datos biométricos.
- La revisión de un caso de aplicación concreta, tanto en lo que respecta al cumplimiento de normas y reglamentaciones en vigencia, cuanto a la selección y uso de cuáles tecnologías.
- El estudio de las tecnologías disponibles para dicho propósito, impuestas o no por el marco normativo.

Para su desarrollo, a los efectos de alcanzar los objetivos señalados y verificar, o no, las hipótesis planteadas, el trabajo se estructura en los siguientes capítulos:

1.5.4.1. Estudio del marco normativo

En este capítulo se realiza una compilación de las normas vigentes más relevantes en relación con la protección de datos personales en el ámbito nacional argentino, con detalle del alcance y un extracto de los principales cometidos de cada norma identificada. Este compilado se realiza de manera introductoria sobre la protección de datos personales en general, mientras que se particulariza ciertos aspectos que refieren a datos biométricos y a las condiciones de seguridad sobre la integración y almacenamiento de archivos, bases de datos o registros.

Asimismo, el capítulo referencia un anexo que pormenoriza las normas por tipo, nivel y alcance de cada una, fecha de dictado y detalle de los principales contenidos.

En segundo término, se analizan los rasgos más destacados del marco normativo en su conjunto y los aportes sustantivos de cada norma al mismo, a los efectos de realizar una valoración del marco normativo descripto, conforme determinados criterios de efectividad y cobertura.

Finalmente, se contrasta la valoración obtenida con las características distintivas del proyecto de nueva ley de protección de datos personales enviado al Congreso Nacional por el Poder Ejecutivo en septiembre de 2018. Asimismo, cabe aclarar que recientemente, al inicio del período legislativo de sesiones ordinarias del presente año, período N° 138 (marzo 2020 - febrero 2021) el proyecto ha perdido estado de trámite parlamentario. No se conoce por el momento el interés que pueda existir por parte de las actuales autoridades políticas para impulsarlo nuevamente o presentar otro diferente.

1.5.4.2. Estudio del sistema Mi Huella o SBA

En este capítulo se incluye como caso de estudio en relación con las hipótesis sustentadas, al sistema de identificación biométrica de la ANSES, Administración Nacional de la Seguridad Social, denominado formalmente por este organismo como Sistema de Identificación Biométrica de ANSES o SBA y divulgado (y reconocido por sus usuarios) con el nombre de Mi Huella.

El estudio se desarrolla a partir de recabar los antecedentes jurídicos e institucionales del sistema, los cuales incluyen una solicitud a la ANSES de información técnica específica sobre el sistema referido.

Con la información obtenida, se procede a exponer el conjunto de normas de aplicación sobre el sistema, a los efectos de conocer el marco normativo específico. Luego se realiza una valoración de las normas, reglamentos y de la tecnología apropiada por Mi Huella, tanto en relación con la protección de los datos biométricos en general, como respecto del almacenamiento y de la conservación de los mismos.

1.5.4.3. Revisión de las tecnologías disponibles y utilizadas

El capítulo realiza en primer término una introducción pormenorizada a las tecnologías de los sistemas automatizados de huellas dactilares (AFIS es la sigla con la que se los conoce). En la misma se incursiona en los aspectos y características tecnológicas de los diferentes factores, elementos o fases de los AFIS, a saber:

- Adquisición de la imagen y su digitalización.
- Extracción de características o de las singularidades de las crestas de huellas dactilares, comúnmente conocidas como puntos de minucia.
- Aspectos ligados al proceso de emparejamiento o de comparación entre huellas y factores de indexación y recuperación

En un segundo apartado, se analiza la tecnología propietaria Megamatcher, dado que es la utilizada por el sistema de ANSES Mi Huella. Para ello se presentan los principales antecedentes y rasgos de la misma, así como una revisión de sus principales componentes y los diseños de arquitectura con los que se ofrece en el mercado actual.

Finalmente, en relación con Megamatcher, se realiza una valoración acerca de las medidas de recuperación de incidencias o desastres que la firma propietaria pone a disposición de sus usuarios.

La tercera parte del capítulo está dedicada a una revisión sobre las tecnologías de almacenamiento de datos biométricos recientemente impulsadas por la Unión Europea. Con ese propósito se analiza un documento que presenta una propuesta de reglamento de interoperabilidad de sistemas orientados a la gestión de migraciones, control de fronteras y seguridad. Este documento adquiere relevancia en el contexto del presente trabajo por cuanto su núcleo es un sistema de identificación biométrica. A partir de él, es posible apreciar cuáles son las premisas fundamentales a tener en cuenta sobre el tratamiento y almacenamiento de los datos biométricos, así como describir y valorar de alguna manera las medidas y prácticas de seguridad insertas en el reglamento y en particular sobre el sistema compartido biométrico que está en su núcleo.

La cuarta y última parte del capítulo trata sobre las conclusiones preliminares que pueden obtenerse respecto de las tecnologías biométricas actuales.

1.5.4.4. Conclusiones, recomendaciones y pasos a seguir

El último capítulo sustantivo está dedicado a interpretar la información obtenida y analizada respecto de los aspectos normativos y los tecnológicos, en el marco de una validación de las hipótesis sustentadas por el trabajo. En particular, en relación con el ajuste al marco normativo y los riesgos de inadecuada o insuficiente protección que entrañan las tecnologías en uso en Argentina, así como la posibilidad de mejora que podría darse al adoptar otras disponibles.

Asimismo, se valoran las tecnologías de almacenamiento de datos biométricos en Mi Huella y la pertinencia o factibilidad de aplicar otras nuevas, diferentes o complementarias.

La redacción de conclusiones se efectúa entonces en términos de validación de las hipótesis del trabajo, de ratificación de los principales aportes logrados, de enunciado de posibles aportes futuros o recomendaciones, así como, principalmente, a los efectos de demostrar el cumplimiento de los objetivos propuestos al inicio de este trabajo.

Capítulo II – ESTUDIO DEL MARCO NORMATIVO

2.1. Introducción

El presente capítulo ofrece en primer término una compilación de las normas vigentes más relevantes en relación con la protección de datos personales en el ámbito nacional argentino. Con dicho objeto se presenta una tabla resumen que enuncia y explica el alcance y los principales cometidos de cada norma identificada, al tiempo que se agrega un anexo con mayor nivel de detalle: Tipo, nivel y alcance de cada norma, fecha de dictado, principales contenidos.

En segundo término, se analizan los rasgos más destacados del marco normativo en su conjunto y los aportes sustantivos de cada norma a esta caracterización que se plantea. Cabe destacar que el enfoque es introductorio

sobre la protección de datos personales en general a la vez que pretende volverse particularizado respecto de ciertos aspectos que refieren a datos biométricos y a las condiciones de seguridad sobre la integración y almacenamiento de archivos, bases de datos o registros.

Seguidamente se plantea una valoración del marco normativo descripto, conforme determinados criterios de efectividad y cobertura.

Por fin, en último término, se efectúa un contraste entre esta valoración y las características distintivas del proyecto de nueva ley de protección de datos personales que está a la fecha en trámite parlamentario en el Congreso Nacional.

2.2. Normas identificadas

Ítem	Norma	Objeto principal
1	Ley N° 25.326 Protección de Datos Personales	Dictada a fines del 2000 tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.
2	Decreto 1558 / 2001	Aprueba la reglamentación de la Ley Nº 25.326 que se explaya en su Anexo I.
3	Decreto 1160 / 2010	Modifica inciso 3 de artículo 31 del Anexo I del Decreto Nº 1558/01 dedicado al procedimiento para aplicar sanciones.
4	Ley 27.275 Derecho de Acceso a la Información Pública	Dictada en 2016 tiene por objeto garantizar el efectivo ejercicio del derecho de acceso a la información pública, así como promover la participación ciudadana y la transparencia de la gestión pública. Crea la Agencia de Acceso a la Información Pública AAIP, autoridad de aplicación de la Ley de Protección de Datos Personales.
5	Decreto 206 / 2017	Aprueba la reglamentación de la Ley Nº 27.275.
6	Proyecto Ley Modificatoria Ley 25.326	A la fecha en tratamiento parlamentario. Versión elaborada luego de analizar los aportes y comentarios recibidos durante una consulta pública de febrero de 2017, sobre el anteproyecto de Ley de Protección de Datos Personales generado en el año 2016.
7	Resolución AAIP 4 /2018	Aprueba criterios orientadores de mejores prácticas de la Ley 27.275. Principalmente

Ítem	Norma	Objeto principal
		dirigidos a la efectividad del reclamo.
8	Resolución AIIP 5 /2018	Establece como procedimiento interno de la AAIP, la obligatoriedad de la intervención de la D. Nacional de Datos Personales, dependiente de la misma, en los reclamos por incumplimiento previstos en la ley n° 27.275 que afecten o puedan afectar la protección de datos personales.
9	Resolución AAIP 40 / 2018	Aprueba Política Modelo de Protección de Datos Personales para Organismos Públicos y recomienda a los organismos públicos titulares de bases de datos personales la adopción de la misma o similar, así como su difusión hacia la ciudadanía.
10	Resolución AAIP 47 / 2018	Aprueba Medidas de Seguridad Recomendadas para el Tratamiento y Conservación de Datos Personales en Medios Informatizados como Anexo I. Deroga Disposiciones de la DNPDP N° 11de 2006 y N° 09 de 2008.
11	Resolución AAIP 48 / 2018	Aprueba los criterios orientadores de mejores prácticas en la Ley 27.275.- Principalmente da pautas para la determinación y el entendimiento del INTERÉS PÚBLICO, con la finalidad de elucidar controversias entre el interés público y la vigencia de otros derechos, así como facilitar el trámite de acceso a la información.
12	Resolución AAIP 132 /2018	Sobre la inscripción, modificación y baja de bases de datos a través de TAD o sistema GDE
13	Resolución AAIP 4 / 2019	Criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley Nº 25.326. Define datos biométricos y determina cuándo se considerarán datos sensibles. Además establece pautas para la acreditación del consentimiento del titular respecto de la guarda.
14	Resolución AAIP 86 / 2019	Aprueba GUÍA sobre tratamiento de datos personales con fines electorales.

Tabla 1: Normas identificadas sobre protección de datos de alcance general en ámbito nacional

Para obtener más información sobre cada una de las normas vigentes identificadas, se sugiere consultar el Anexo I.

2.3. Principales características del marco normativo

2.3.1. Ley 25.326 de Protección de Datos Personales

La norma rectora por la cual dar comienzo al estudio es la Ley 25.326 de Protección de Datos Personales (PDP) o de Hábeas Data. Se desprende directamente de lo establecido en el nuevo capítulo titulado “Nuevos Derechos y Garantías”, por medio de la reforma constitucional sancionada en el año 1994. Así se incluyó el artículo 43 cuyo párrafo tercero contempla el llamado habeas data, de la siguiente forma: *Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.*

Se trata de un procedimiento orientado a resguardar la privacidad y el honor o buen nombre de las personas, derechos que podrían verse afectados por las prácticas computacionales que cada vez gravitan con mayor incidencia en la acumulación y en el manejo de una creciente masa de información acerca de la vida de todos los días de cada persona.

Entonces, sin otros antecedentes en el plano nacional, la Ley 25.326 se crea a fin del año 2000 para dar respuesta a la previsión constitucional antedicha, con el objeto de proteger integralmente los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, a los efectos de garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de acuerdo al artículo constitucional referido.

En la instrumentación de ese propósito, la ley realiza una serie de definiciones elementales acerca de los datos personales y sus características y crea una repartición estatal, la Dirección Nacional de Protección de Datos Personales (DNPDP) ubicada originalmente en el entonces Ministerio de Justicia, hoy Ministerio de Justicia y Derechos Humanos, que se constituye en autoridad de aplicación de la ley.

Entre las definiciones básicas que propone la ley (y que en este estudio se reproducen en el glosario) se destacan las siguientes:

- Datos personales.
- Datos sensibles.
- Archivo, registro, base o banco de datos, indistintamente.
- Responsable de archivo, registro, base o banco de datos.
- Titular de los datos.
- Usuario de datos.
- Disociación de datos.

Además, algunos de los principios que se establecen en su capítulo segundo, son clave para entender los pilares del ordenamiento legal a construir en materia de protección de datos personales. Entre ellos:

- Inscripción: La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos ante la autoridad de aplicación.
- Exactitud y actualización: Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. Los datos total o parcialmente inexactos o incompletos, deben ser suprimidos, sustituidos o completados, por el responsable del archivo, sin perjuicio de los derechos del titular.
- Almacenamiento: Deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular y debe ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.
- Consentimiento: El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar formalmente.
- Deber de seguridad y de confidencialidad: El responsable o el usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado.
- Restricciones a la cesión o transferencia de datos: En principio, los datos personales sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento expreso del titular de los datos. Asimismo está prohibida la transferencia de datos a países u organismos internacionales que no cuenten con niveles de protección adecuados.

En sus capítulos siguientes, la ley de PDP contiene las siguientes previsiones:

- Referidas a los derechos de los titulares de los datos:
    - Derecho de información.
    - Derecho de acceso.
    - Derecho de rectificación, actualización o supresión.
    - Excepciones a los anteriores en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.
- Relativas a los usuarios y responsables de archivos, registros y bases de datos:
    - Inscripción de archivos, registros y bases de datos públicos o privados destinados a dar informes.
    - Previsiones específicas para archivos, registros o bancos de datos públicos.
    - Previsiones específicas para archivos, registros o bancos de datos privados con datos de uso no exclusivamente personal.
    - Prestación de servicios informatizados de datos personales.
    - Prestación de servicios de información crediticia.
    - Archivos con fines de publicidad; Archivos relativos a encuestas.
- Respecto de las funciones y atribuciones del órgano de control

En el capítulo VI, la ley se explaya en relación con las sanciones administrativas que van desde el apercibimiento y la suspensión hasta la aplicación de multas y la clausura. Además, avanza con las sanciones penales e introduce nuevos artículos en el Código Penal

- Artículo 117 bis que establece penas por inserción de datos falsos en un archivo de datos personales o por entrega a un tercero a sabiendas de información falsa.
- Artículo 157 bis que determina penas por acceder a sabiendas e ilegítimamente a datos personales o por revelar información confidencial o secreta.
- En ambos casos, la pena se agrava cuando el autor del delito sea un funcionario público.

Finalmente, la ley explica cuándo y cómo procede la acción de protección de los datos personales o de hábeas data para tomar conocimiento de datos personales o para exigir su rectificación, supresión, confidencialidad o actualización cuando se presuma falsedad, inexactitud o caducidad. Explica

además las diferencias entre legitimación activa, es decir la ejercida por el afectado, y legitimación pasiva, que es la llevada a cabo por los responsables y usuarios de bancos de datos.

En líneas generales, la ley instruye que la acción de hábeas data se tramite según lo dispuesto en el cuerpo de la propia ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente, por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.

La reglamentación de la ley de PDP se realizó a través del Decreto 1558/2001, con una modificación menor por medio del Decreto 1160/2010. Como toda reglamentación, produce mayores precisiones sobre el alcance y formas de aplicar la ley. En este caso, se avanza sobre:

- El concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes: son aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.
- Cuestiones de procedimiento relativas al accionar y las competencias de fiscalización de la Dirección Nacional de Protección de Datos Personales.
- Reglamentación específica para la acción de acceso a los datos personales. En particular se indica que no requiere de fórmulas específicas, siempre que garantice la identificación del titular. Así se puede efectuar de manera directa y presencial, o indirecta por medio escrito, electrónico o línea telefónica. En el caso de los archivos o bases de datos públicas conformadas por cesión de información suministrada por entidades financieras, administradoras de fondos de jubilaciones y pensiones y entidades aseguradoras, los derechos de rectificación, actualización, supresión y confidencialidad deben ejercerse ante la entidad cedente del dato impugnado.
- El decreto modificatorio de la reglamentación establece un único artículo por el cual se sustituye un inciso del artículo 31 relativo al procedimiento a seguir para la aplicación de sanciones. Esta modificación contempla las diferentes acciones de la DNPDP, los pasos a seguir, los plazos, las instancias a cubrir y los recursos a considerar hasta la resolución en firme y su ingreso al Registro de Infractores que lleva la DNPDP.

2.3.2. Ley 27.275 Derecho de Acceso a la Información Pública

En septiembre de 2016 se sanciona la Ley 27.275 de Derecho de Acceso a la Información Pública (AIP) con el objeto de garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover la participación ciudadana y la transparencia de la gestión pública.

Uno de los principios en los que se basa es el de la presunción de publicidad, lo cual significa que toda la información en poder del Estado se presume pública, salvo las excepciones previstas por la propia ley. Precisamente, una de las excepciones más importantes es cuando la información refiere o contiene datos personales que deben ser protegidos.

De esta manera, a pesar de ser la ley de AIP posterior en el tiempo (más de 15 años) ella se transforma en la regla y la de PDP, de alguna manera, en la excepción. En rigor, la PDP es una de las excepciones expresamente contempladas en el artículo 8 de la ley, a través de dos incisos, el primero genérico y el segundo bien específico:

- Inciso d) Información que comprometa los derechos o intereses legítimos de un tercero obtenida en carácter confidencial;
- Inciso i) Información que contenga datos personales y no pueda brindarse aplicando procedimientos de disociación, salvo que se cumpla con las condiciones de licitud previstas en la ley 25.326 de protección de datos personales y sus modificatorias;

Además, lo anterior no es el único vínculo a tomar en cuenta. A mediados del año 2017, por medio del Decreto N° 746 /2017, la Agencia de Acceso a la Información Pública se transforma en el órgano de control de la Ley Nº 25.326 y por ello, desde ese momento, incorpora dentro de sus dependencias a la Dirección Nacional de Protección de Datos Personales, la cual funciona en la práctica como la primera instancia legal y técnica para la aplicación de la ley, reservando el nivel resolutorio a la propia AAIP.

Otros principios de la ley de AIP que resulta de interés destacar para un análisis compresivo y pormenorizado:

- **Transparencia y máxima divulgación**: toda la información en poder, custodia o bajo control del sujeto obligado debe ser accesible para todas las personas, salvo excepciones fundadas.
- **Máximo acceso**: la información debe publicarse de forma completa, con el mayor nivel de desagregación posible y por la mayor cantidad de medios disponibles.
- **Apertura**: la información debe ser accesible en formatos electrónicos abiertos, que faciliten su procesamiento por medios automáticos que permitan su reutilización o su redistribución por parte de terceros.
- **Control**: el cumplimiento de las normas que regulan el derecho de acceso a la información será objeto de fiscalización permanente. Las resoluciones que denieguen solicitudes de acceso a la información, como el silencio del sujeto obligado requerido, la ambigüedad o la inexactitud de su repuesta, podrán ser recurridas ante el órgano competente.
- **Alcance limitado de las excepciones**: los límites al derecho de acceso a la información pública deben ser excepcionales, quedando la responsabilidad de demostrar la validez de cualquier restricción al acceso a la información a cargo del sujeto al que se le requiere la información.
- **In dubio pro petitor**: la interpretación de las disposiciones de esta ley o de cualquier reglamentación del derecho de acceso a la información debe ser efectuada, en caso de duda, siempre en favor de la mayor vigencia y alcance del derecho a la información.

También se enuncia un **principio de disociación** que refiere a que cuando parte de la información se encuadre dentro de las excepciones taxativamente establecidas por esta ley, la información no exceptuada debe ser publicada en una versión del documento que tache, oculte o disocie aquellas partes sujetas a la excepción.

La definición de disociación había sido dada por la ley de PDP, sin embargo es en el contexto de la ley de AIP cuando adquiere nitidez.

Asimismo, a través del principio de disociación y de todos los citados previamente queda en claro que la protección de los datos personales no está menoscabada por el nuevo cuerpo legal sino que se exige a los sujetos obligados que extremen los recaudos para satisfacer las demandas de información pública sin afectar los derechos de las personas en relación con sus datos personales.

El derecho de acceso a la información pública comprende la posibilidad de buscar, acceder, solicitar, recibir, copiar, analizar, reprocesar, reutilizar y

redistribuir libremente la información bajo custodia de los sujetos obligados, con las únicas limitaciones y excepciones establecidas.

Toda persona humana o jurídica, pública o privada, tiene derecho a solicitar y recibir información pública, no pudiendo exigirse al solicitante que motive la solicitud, que acredite derecho subjetivo o interés legítimo o que cuente con patrocinio letrado.

Se presume pública toda información que generen, obtengan, transformen, controlen o custodien los sujetos obligados alcanzados por esta ley.

En cuanto a los sujetos obligados, la ley expresa taxativamente quiénes son en su artículo 7°. Dicho de una manera simple, se trata de los organismos de la administración pública nacional y de los demás poderes constitucionales, así como la parte estatal de empresas y sociedades del Estado; concesionarios, permisionarios y licenciatarios de servicios públicos y toda entidad pública o privada que maneje fondos públicos por la parte que alcance a estos.

La ley hace un aporte sustantivo en lo que respecta a la instrumentación de la solicitud de la información y las vías de reclamo. Para ello, a través de varios artículos de su capítulo III se explaya sobre las formas de la solicitud de información (incluso encomienda que se ponga en marcha una plataforma para la solicitud y su trámite digital a través de la web), su tramitación, plazos, respuestas a propiciar en el caso de información parcial, casos de denegatoria, vías de reclamo, procedimiento del reclamo por incumplimiento, sus requisitos formales, cómo se resuelve el reclamo interpuesto y cuáles son las responsabilidades en juego.

También es de interés la construcción institucional que la ley realiza en el caso de la Agencia de Acceso a la Información Pública, la cual no es sólo la autoridad de aplicación de la ley de AIP sino también, como órgano rector, de la ley de PDP.

En el capítulo IV se explican las pautas de organicidad de la AAIP relativas a su creación, órgano de dirección, rango y jerarquía del director, procedimiento de selección del director, requisitos e incompatibilidades; rango y jerarquía del mismo y mecanismos de remoción y cese. Dentro de las competencias y funciones asignadas al director, se destacan las siguientes:

- Redactar y aprobar el Reglamento de Acceso a la Información Pública aplicable a todos los sujetos obligados;
- Implementar una plataforma tecnológica para la gestión de las solicitudes de información y sus correspondientes respuestas;
- Requerir a los sujetos obligados que modifiquen o adecuen su organización, procedimientos, sistemas de atención al público y recepción de correspondencia a la normativa aplicable a los fines de cumplir con el objeto de la presente ley;
- Elaborar criterios orientadores e indicadores de mejores prácticas destinados a los sujetos obligados;
- Elaborar y presentar ante el Honorable Congreso de la Nación propuestas de reforma legislativa respecto de su área de competencia;
- Solicitar a los sujetos obligados expedientes, informes, documentos, antecedentes y cualquier otro elemento necesario a los efectos de ejercer su labor;
- Recibir y resolver los reclamos administrativos que interpongan los solicitantes de información pública y publicar las resoluciones que se dicten en ese marco;
- Promover las acciones judiciales que correspondan, para lo cual la Agencia de Acceso a la Información Pública tiene legitimación procesal activa en el marco de su competencia;
- Impulsar las sanciones administrativas pertinentes ante las autoridades competentes correspondientes en los casos de incumplimiento a lo establecido en la presente ley;
- Publicar los índices de información reservada elaborados por los sujetos obligados.

Además, la ley impone un plazo para la creación de organismos similares en el seno del Poder Judicial de la Nación, del Ministerio Público Fiscal de la Nación, del Ministerio Público de la Defensa y del Consejo de la Magistratura.

También, siempre dentro de la nueva construcción institucional, crea el Consejo Federal para la Transparencia, como un organismo inter jurisdiccional de carácter permanente, que tendrá por objeto la cooperación técnica y la concertación de políticas en materia de transparencia y acceso a la información pública.

A su vez, la ley dispone que cada uno de los sujetos obligados nombre a un responsable de acceso a la información pública a los efectos de que reciba, tramite y dé seguimiento a las solicitudes de acceso a la información pública dentro de su jurisdicción. Estos responsables también deben promover la

implementación de las resoluciones elaboradas por AAIP y prácticas de transparencia en la gestión pública, así como publicar, en caso de corresponder, la información que hubiese sido desclasificada;

Dentro de lo que la ley denomina una política de transparencia activa, se señala que los sujetos obligados deberán facilitar la búsqueda y el acceso a la información pública a través de su página oficial de la red informática, de una manera clara, estructurada y entendible para los interesados, procurando accesibilidad y la reutilización de la información por parte de terceros. Se aclara que serán de aplicación, en su caso, las excepciones al derecho de acceso a la información pública y, especialmente, la referida a la información que contenga datos personales.

2.3.3. Resoluciones de la AIIP y disposiciones de la DNPDP

Dentro de las resoluciones y disposiciones vigentes de los organismos técnicos y rectores centrales, es decir la AIIP y su DNPDP, se destacan las siguientes, en orden de acuerdo a la cronología de su emisión:

1. La Resolución E 4/2018 de la AAIP por la cual se aprueban criterios orientadores de mejores prácticas de la Ley de AIP, sobre todo dirigidos a la efectividad del reclamo y a la advertencia o sanción de incumplimientos.
2. La Resolución E 5/2018 de la AAIP por la que se establece la obligatoriedad de la intervención de la DNPDP como procedimiento interno de la AAIP en los reclamos por incumplimiento de acceso a la información pública que puedan afectar la protección de datos personales. En tales casos, la Dirección referida deberá expedirse con un informe al respecto.
3. La Política Modelo de protección de datos personales recomendada para organismos públicos, aprobada por Resolución 40/2018 de la AAIP. A través de ella se sugiere a los titulares de bases de datos personales la adopción de un conjunto de pautas y de procedimientos referidos a la protección así como su difusión hacia la ciudadanía. Asimismo recomienda que en cada organismo público se realice la designación de un agente de planta como delegado de protección de

datos personales, para que se responsabilice por la implementación y el control de cumplimiento interno de la política adoptada.

La Política impulsa un conjunto de declaraciones que los organismos deberían adoptar en relación con el tratamiento de datos personales, haciéndole saber al ciudadano cómo opera cada institución respecto de:

- Cuáles son los datos personales que el organismo maneja, en qué bases de datos, con qué finalidad y cómo han sido éstas inscriptas, de acuerdo a lo estipulado por la ley de PDP.
- Qué pautas o procedimientos se han adoptado en relación con la caducidad, confidencialidad y seguridad de los datos, así como respecto del tratamiento de riesgos asociados a su adulteración, pérdida, consulta o tratamiento no autorizado.

Cabe destacar que la Política indica que, en caso de detectarse un incidente de seguridad que implique un riesgo significativo para el titular del dato, se comunicará sin dilación tal evento a la DNPDP de la AAIP, señalando así la gravedad que se le atribuye al proceso de protección.

No obstante, la Política Modelo no establece el alcance, las formas o los métodos ni la profundidad de las medidas de protección que deberían declararse adoptadas.

4. Resolución 47/2018 de la AAIP por la que se aprueba medidas de seguridad recomendadas para el tratamiento y conservación de datos personales en medios informatizados (en el Anexo I de la resolución) en atención a la evolución vertiginosa de la tecnología e internet, como así también las redes sociales, los servicios de mensajería instantánea y el comercio a través de la red. Además, por ese mismo motivo, la resolución deroga disposiciones anteriores de la DNPDP sobre la materia (N° 11 de 2006 y N° 09 de 2008).

   A fin de adecuarse a las nuevas tecnologías, la resolución, a través de su Anexo I establece de modo referencial y esquemático, con el objetivo de facilitar el cumplimiento de la Ley de PDP, las medidas de seguridad recomendadas para la administración, planificación, control y mejora continua de la seguridad de la información, para cada uno de los procesos, tareas y especialidades que las entidades desarrollen en

cuanto a la recolección de datos, el control de acceso, el control de cambios y la gestión de vulnerabilidades. Respecto del almacenamiento, el registro o la conservación de los datos, no hay prácticamente referencia alguna.

5. Resolución 48/2018 de la AAIP por la cual se aprueban los criterios orientadores de mejores prácticas en la aplicación de la ley de AIP. A través de tales criterios se dan pautas para la determinación y el entendimiento de qué es y cuándo hay interés público, a los fines de elucidar controversias entre el mismo y la vigencia de otros derechos, así como para facilitar el trámite de acceso a la información. Inclusive un criterio específicamente orienta acerca de cómo cursar una solicitud de acceso a la información pública en relación con los datos personales que tenga un organismo obligado.
6. La Resolución 4 / 2019 de la AAIP aprueba criterios orientadores e indicadores de mejores prácticas en la aplicación de la ley de PDP. A los efectos de modernizar la legislación y adaptarse a las nuevas tecnologías de la era digital, la resolución define a los datos biométricos como aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única. Además, determina que los datos biométricos se considerarán datos sensibles únicamente cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su titular.

   Otro criterio avanza sobre el derecho de acceso en relación a datos personales que han sido recolectados mediante sistemas de video vigilancia. También, en atención a que los cambios tecnológicos han permitido automatizar el tratamiento de datos y que ello podría acarrear riesgos a la persona, la AAIP considera importante establecer cuál sería el alcance del derecho de acceso del titular de los datos cuando el responsable de la base de datos tome decisiones basadas únicamente en el tratamiento automatizado de datos.

Otros criterios establecen pautas para la acreditación del consentimiento del titular respecto de la guarda.

2.4. Análisis valorativo del marco normativo vigente

2.4.1. Análisis respecto de la cobertura

En primer término se hace una valoración de las normas en vigencia con respecto del alcance, amplitud y cobertura del fenómeno de la protección de los datos personales.

En ese sentido, indudablemente, la Ley de Protección de Datos Personales recoge un mandato constitucional al crear el instituto del hábeas data para la subordinación del manejo de datos personales por parte de terceros, al resguardo de la privacidad y del honor de cada persona.

Dicho cuerpo legal está orientado en su aplicación a los bancos de datos públicos y del sistema de la previsión social, los del sector financiero (bancos, entidades financieras, compañías aseguradoras) y los del sector de la salud. No obstante la extensión o amplitud que aparentemente incorpora la reglamentación en el concepto de archivos, registros o bancos de datos, en la práctica no parece haber una mayor incidencia en bases de datos personales de origen o finalidad privadas (por ejemplo, los registros de datos de afiliación de instituciones deportivas o educativas privadas, datos de clientes de empresas privadas de servicios no públicos, etc.) privadas.

Sobre aspectos vinculados al almacenamiento (medios, métodos, formas, medidas de protección) la ley PDP no se explaya de ninguna manera, sólo hay una mención muy general en relación con la seguridad o la preservación de la integridad y la confidencialidad de los bancos de datos y de quién es la responsabilidad. Este déficit se cubre débilmente con las guías emitidas con carácter de resolución por parte de la AAIP. Son de ayuda al considerar la cuestión de la evolución tecnológica que señalan como vertiginoso, pero resultan insuficientes en los hechos, sobre todo en relación con la diversidad tecnológica que pretenden abarcar.

La ley no distingue a los datos biométricos dentro de los datos personales y si bien este concepto aparece recientemente tratado en una de las guías de criterios orientadores, no se abunda en ninguna cuestión relacionada con su tratamiento, derecho de acceso, almacenamiento o conservación. No obstante, cabe destacar que la distinción de los datos biométricos dentro del cuerpo normativo obedece a la necesidad de modernizar la legislación incorporando elementos que la tecnología impone.

Es evidente que los riesgos relacionados con un archivo o banco de datos digital que se accede por internet o que está alojado en la nube computacional, son muy diferentes a los que podrían asociarse con un registro centralizado en una PC aislada de su entorno. Tampoco los riesgos sobre datos biométricos son similares a los riesgos sobre datos personales no biométricos, ya se explicó esa diferencia y es precisamente la que da fundamento a gran parte del presente estudio.

Las medidas de seguridad recomendadas para la administración, planificación, control y mejora continua de la seguridad de la información en cada uno de los procesos, tareas y especialidades habituales en las entidades tratantes de datos personales se refieren a la recolección de datos, al control de accesos, al control de cambios de los sistemas y aplicaciones y a la gestión de vulnerabilidades. Todo ello a través de una de las guías emanadas de la AAIP, porque la ley de PDP y su reglamentación por decreto no mencionan elementos o instrumentos especialmente dedicados a la seguridad, integridad o protección de los datos. Además, respecto del almacenamiento, el registro o la conservación de los datos, no hay prácticamente referencia alguna en todo el cuerpo normativo.

2.4.2. Análisis respecto de la efectividad

Cabe señalar que se entiende el concepto de efectividad como un criterio que permita discernir qué tan obligada está la sociedad y en particular uno de los actores protagónicos de la protección de datos, el responsable de bases o bancos de datos, al cumplimiento de la ley.

En primer término es posible señalar que la ley de AIP que se sucede a la de PDP y de alguna manera es instrumentadora de ésta, aporta mayor efectividad a los procedimientos del conjunto, es decir, a la posibilidad de poner en ejecución

las previsiones de la ley para la tutela de los derechos de los titulares sobre sus datos personales.

Esta mayor efectividad puede apreciarse, por un lado, por la elevación del rango institucional del organismo que tutela ambas legislaciones. En la práctica se da un virtual ascenso del organismo de control de la aplicación del régimen legal: de una dirección nacional en la órbita de una cartera de Estado a una agencia estatal inserta en la Jefatura de Gabinete de Ministros. Una agencia que goza de una cierta autonomía tanto por el diseño de sus competencias, atribuciones o facultades (regulatorias, complementarias en lo legislativo, interpretativas, fiscalizadoras y sancionadoras) como por cuáles son las reglas para la cobertura de los cargos de responsabilidad, con avales y requisitos especiales, así como los mecanismos de remoción previstos.

Por otro lado, contribuye grandemente a una mayor efectividad el conjunto de criterios y guías de procedimientos que despliega la AAIP. La Agencia instrumenta y facilita sobre todo el procedimiento de acceso a la información pública y luego avanza sobre el ejercicio del derecho de acceso a los datos personales (el recurso de hábeas data) asimilándolo a un caso en particular de las solicitudes de acceso a la información pública, invocando el art. 14 de la ley de PDP. Así aprovecha todo el andamiaje montado para AIP también en el caso de la PDP. Se trata de un conjunto de recursos nada desdeñable. Por el contrario, involucra agentes coordinadores y responsables en cada jurisdicción u organismo para dar respuesta a las solicitudes, mecanismos de tramitación a distancia y manuales de procedimientos que establecen pasos, responsables, tareas y plazos.

Cabe señalar que la sanción del Reglamento General de Protección de Datos (o más conocido como GDPR por sus siglas en inglés) trascendió la frontera de la Unión Europea de tal forma que desde su sanción, Argentina (entre otros países) comenzó un proceso de actualización del régimen de datos personales. Es en este marco que se publicó la Resolución N° 4/2019, por la cual

se aprobaron los criterios orientadores e indicadores de mejores prácticas en la aplicación de la ley de PDP. [5].

Entre dicho proceso se puede mencionar el hecho de que se encuentra bajo tratamiento por el Congreso de la Nación un proyecto de modificación de la actual Ley N° 25.326 de Protección de Datos Personales (LPDP) y la emisión de nueva reglamentación por parte de la Agencia de Acceso a la Información Pública.

Otro aspecto que refuerza la efectividad del cuerpo normativo es que el régimen de control de cumplimiento y eventual aplicación de sanciones que está determinado en sus conceptos desde la ley de PDP, se mejora a través de una modificación de su decreto reglamentario en el año 2010 y se termina de robustecer desde el accionar sistemático de la AAIP como órgano de control y resolución de recursos y descargos.

Una apreciación directa del sitio oficial de AAIP (https://www.argentina.gob.ar/aaip) permite observar algunos aspectos relevantes.

Figura 1 Imagen página oficial de AAIP/PDP

Dentro de los trámites y servicios destacados, se pone en evidencia el grado de instrucción y completitud de la información orientada al ciudadano y al

[5] Ref. Bibliográfica [5] 8° Encuentro Nacional de Seguridad de la Información & Ciberseguridad.19 https://www.forosyconferencias.com.ar/evento/Seguridad_de_la_Informacion

responsable de bases o banco de datos. Las acciones más relevantes previstas por la legislación están facilitadas por cuestionarios o guías como en el ejemplo ilustrado a continuación.

Derecho de rectificación, actualización o supresión

Si una empresa u organismo público posee datos tuyos erróneos, podés solicitarle que los actualicen o rectifiquen o supriman y que, mientras dure el proceso de verificación, los bloquee o informe que se encuentran sometidos a revisión.

¿Cómo lo solicito?

Hacé el pedido al organismo público, empresa o profesional que posee tus datos.

DESCARGÁ EL MODELO DE SOLICITUD DE RECTIFICACIÓN,ACTUALIZACIÓN O SUPRESIÓN

¿En cuánto tiempo deben responderme?

Una vez que reciben tu solicitud, tienen 5 días hábiles para realizar la supresión, actualización o rectificación.

¿Qué hago si no me responden o si la información que me brindan es insuficiente?

Vencido el plazo, podés:
Denunciarlo ante la Dirección Nacional de Protección de Datos Personales de la Agencia de Acceso a la Información Pública o realizar una presentación judicial, acción de Habeas Data.

¿Cómo hago la denuncia ante la Dirección Nacional de Protección de Datos Personales?

El procedimiento es el mismo que en el caso de una denuncia por incumplimiento del Derecho de acceso.

Figura 2 Ejemplo de instructivo en página oficial de AAIP / PDP

También resulta de cierto interés apreciar la efectividad del aparato legal al momento de determinar y aplicar sanciones ante reclamos por incumplimiento. Para ello, se han cotejado las resoluciones publicadas en el sitio oficial de AAIP (https://www.argentina.gob.ar/aaip/buscador-normativa), tanto en firme como en alguna instancia recursiva, es decir no firme. Los resultados indican que de aproximadamente 80 resoluciones registradas en dicho sitio desde agosto de 2018, cuya sustancia es la aplicación de una sanción pecuniaria, situación terminal en el tramo administrativo ante la constatación de un incumplimiento en la protección de datos personales, solamente una está en firme y aparentemente por vencimiento del plazo para interponer algún recurso.

Este análisis superficial permite, sin embargo, conjeturar que el proceso sancionatorio, como instancia final del ejercicio del poder fiscalizador de la AAIP, es poco efectivo o al menos demasiado trabajoso o demasiado lento.

2.4.3. Aportes del proyecto de modificación de ley en trámite

Tal como se señaló anteriormente, Argentina no fue ajena al proceso de actualización del régimen de datos personales devenido en muchos países a partir de la sanción del GDPR por parte de la Unión Europea. En esta línea de trabajo se inscribieron las principales cuestiones planteadas o directamente resueltas por la vía de la reglamentación a través de la AAIP y sobre todo, por el proyecto de ley modificatoria de la N° 25.326 de PDP que se encuentra actualmente bajo tratamiento del Congreso de la Nación.

Es de gran interés apreciar cuáles son los aspectos que recoge la nueva legislación, ya sea que se trate de cuestiones introducidas por la reglamentación en los últimos tiempos y que requieren integrarse al cuerpo normativo para dotar de mayor fortaleza al conjunto, o que impliquen aspectos impulsados por la innovación tecnológica y hasta ahora no tratados.

Desde la sanción de la Ley N° 25.326 la tecnología ha venido evolucionado a un ritmo vertiginoso, impactando en gran medida en la protección de los datos personales y trayendo enormes desafíos en el campo del ejercicio de los derechos. Por un lado, beneficios innegables y por el otro, riesgos sobre la privacidad cada vez más acuciantes. [6]

En líneas generales, el proyecto de ley garantiza los derechos de los titulares de los datos, aclara cuáles son las bases legales para el tratamiento de datos, añade el interés legítimo del responsable del tratamiento, entre otras bases legales, al consentimiento del titular de los datos ya legislado y genera obligaciones a los responsables del tratamiento de datos que son consistentes con el objeto de la norma proyectada: la protección integral de los datos personales a fin de garantizar el ejercicio pleno de los derechos de sus titulares.

En la elaboración de la norma proyectada se ha seguido la tendencia internacional en la materia, estableciendo que la normativa se aplicará en distintos supuestos, aun cuando, bajo ciertas condiciones, los responsables de tratar los datos no se encuentren en territorio nacional. Por otra parte, se dispone que la aplicación de la ley no obstaculizará al tratamiento de datos que realicen los

[6] Ref. Bibliográfica [6] Cuadro comparativo Ley 25.326 de Protección de Datos Personales y Mensaje 147/2018 Proyecto de Ley de Protección de Datos Personales.
https://www.argentina.gob.ar/sites/default/files/comparativo_ley_datos.pdf

medios de comunicación en el ejercicio de la libertad de expresión (aspecto que ya está comprendido en la legislación actual, pero que el proyecto de alguna manera realza).

Asimismo, el proyecto incorpora obligaciones para los responsables del tratamiento no contempladas en la ley vigente, entre otras:

- la obligación de notificar incidentes de seguridad;
- la obligación de realizar una evaluación del impacto relativa a la protección de los datos personales cuando sea probable que entrañe un alto riesgo de afectación a los derechos de los titulares de los datos;
- la obligación de adoptar medidas para el cumplimiento de la ley que sean proporcionales a las modalidades y finalidades del tratamiento de datos, su contexto, el tipo y categoría de datos tratados, y el riesgo que el referido tratamiento pueda acarrear.

Además, se crea la figura del delegado de protección de datos cuya designación es obligatoria en el caso de autoridades u organismos públicos, en el de tratamiento de datos sensibles como parte de la actividad principal del responsable y en el tratamiento de datos a gran escala.

Por otro lado, el proyecto de ley da cabida a derechos de los titulares de los datos que hasta ahora no habían sido reconocidos:

- Derecho a la portabilidad de datos.
- Derecho de los titulares de los datos a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos.
- Derecho a solicitar la supresión de sus datos personales de las bases de datos (bajo ciertas circunstancias y siempre que la supresión no se oponga al ejercicio de la libertad de expresión e información).
- También se incorporan parámetros especiales para el tratamiento de datos de niñas, niños y adolescentes, en el marco del respeto a la Convención sobre los Derechos del Niño.

En relación con aspectos vinculados al almacenamiento, registro o conservación de los datos, el proyecto avanza en algunas cuestiones que impactan de manera directa o indirecta en ellos. En particular resulta de interés lo tratado en los nuevos artículos 19, 20, 33, 37, 40, 41 y 42.

A través del proyectado artículo 19 se establece un nuevo principio de seguridad de los datos personales que señala que el responsable del tratamiento y, en su caso, el encargado, deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y la confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o

tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Además, el responsable del tratamiento debe adoptar las medidas de seguridad aplicables a los datos personales que trate, considerando, al menos, los siguientes factores:

a. El riesgo inherente por el tipo de dato personal;
b. El carácter sensible de los datos personales tratados;
c. El desarrollo tecnológico;
d. Las posibles consecuencias de un incidente de seguridad para los titulares de los datos;
e. Los incidentes de seguridad previos ocurridos en los sistemas de tratamiento.

En el sentido de la enumeración precedente, se puede argumentar que si bien el proyecto no menciona expresamente a los datos biométricos, estos factores comprenderían algunas de sus distinciones y gran parte de su problemática.

Por otra parte, el proyectado artículo 20 trata sobre la notificación de incidentes de seguridad en datos personales, estableciendo que en caso de que ocurra un incidente de seguridad de datos personales, el responsable del tratamiento debe notificarlo a la autoridad de control sin dilación indebida y, de ser posible, dentro de las setenta y dos horas. De igual manera, el responsable del tratamiento también debe informar al titular de los datos sobre el incidente de seguridad ocurrido, en un lenguaje claro y sencillo, cuando sea probable que entrañe altos riesgos a sus derechos. Además, el responsable del tratamiento debe documentar todo incidente de seguridad que ponga en alto riesgo los derechos de los titulares de los datos personales ocurrido en cualquier fase del tratamiento de datos e identificar, de manera enunciativa pero no limitativa, la fecha en que ocurrió, el motivo del incidente, los hechos relacionados con éste y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva.

El artículo 33 del proyecto enuncia el derecho a la portabilidad de datos personales. Si se brindan servicios en forma electrónica que incluyan el tratamiento de datos personales, el titular de los datos tiene derecho a obtener del

responsable del tratamiento una copia de los datos personales objeto de tratamiento en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización. El titular de los datos puede solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.

Si bien el proyecto ya plantea excepciones, queda en claro que en el caso de datos biométricos este artículo deberá ser reglamentado para dar una mayor precisión a sus alcances. Más aún cuando el proyecto de ley no distingue los datos biométricos como un tipo en especial.

Las obligaciones del responsable y del encargado del tratamiento de datos personales establecidas en el proyectado artículo 37 implican medidas más concretas para el cumplimiento de la responsabilidad de una manera proactiva a la vez que amplían el espectro de control, sobre todo a partir de la realización de supervisiones o auditorías, internas o externas, las demostraciones necesarias ante los requerimientos de la autoridad de control y la adopción de políticas de privacidad o de mecanismos de autorregulación vinculantes.

El artículo 38 establece criterios de protección de datos desde el diseño y por defecto. Se trata de dos conceptos que extreman las medidas tecnológicas y organizativas apropiadas tanto con anterioridad como durante el tratamiento de datos a fin de cumplir los principios y los derechos de los titulares de los datos establecidos en la ley. Esta obligación se aplica a la cantidad y calidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas deben garantizar en particular que, por defecto, los datos personales no sean accesibles, sin la intervención del titular de los datos, a un número indeterminado de personas humanas.

El artículo 40 del proyecto determina la necesidad de llevar a cabo una evaluación de impacto relativa a la protección de datos personales por parte del responsable del tratamiento, cuando éste prevea realizar algún tipo de tratamiento que por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación a los derechos de los titulares de los datos. A su vez, y sin perjuicio de otros que establezca la autoridad de control, la evaluación de impacto será obligatoria en los casos de evaluación sistemática y exhaustiva de aspectos personales de personas humanas como la elaboración de perfiles,

tratamiento de datos sensibles a gran escala o de datos relativos a antecedentes penales o contravencionales.

Este último conjunto encierra sin lugar a dudas a datos de tipo biométrico, con lo cual queda en claro que están comprendidos en los alcances de esta previsión.

Luego, a través del artículo 41, se establecen los contenidos mínimos de la evaluación y por medio del artículo 42 se determina que el responsable del tratamiento deberá informar previamente a la autoridad de control en los casos en los que la evaluación de impacto muestre un alto riesgo en el tratamiento proyectado. Los contenidos mínimos de la evaluación de impacto implican:

- Una descripción sistemática de las operaciones de tratamiento de datos previstas y de los fines del tratamiento e interés legítimo perseguido por el responsable.
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento de datos con respecto a su finalidad.
- La evaluación de los riesgos para la protección de los datos personales de los titulares de los datos.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales.

Capítulo ESTUDIO DEL CASO MI HUELLA (SBA)

3.1. Introducción

Tal como fuera señalado en la presentación al comienzo de este trabajo, se incluye como caso de estudio en relación con las hipótesis sustentadas, al sistema de identificación biométrica de la ANSES, Administración Nacional de la Seguridad Social, denominado formalmente por este organismo como Sistema de Identificación Biométrica de ANSES o SBA y divulgado o conocido por sus usuarios con el nombre de Mi Huella.

Si bien ya fue brevemente justificada la inclusión de este caso, es conveniente enunciar a continuación y con mayor grado de detalle, las características que fundamentan su estudio en el contexto del presente trabajo:

- Su objeto principal es el manejo informático de huellas dactilares, uno de los tipos de datos biométricos más utilizados en Argentina y en todo el mundo.
- Concentra una población de individuos titulares de datos biométricos muy elevada. Como indicio de ese gran volumen, es posible señalar que al mes de junio de 2019, el total de titulares de jubilaciones o pensiones contributivas en el nivel nacional de Argentina era de 5.732.758 [7]
- Si bien está regido y utilizado mayormente por ANSES, un organismo del sector público nacional, se extiende al sector privado al involucrar a prácticamente a la totalidad de las entidades financieras y bancarias del país, sus casas centrales y sus sucursales, distribuidas a lo largo y lo ancho de la Argentina.
- Por lo anterior, expone un enorme despliegue territorial además de una compleja trama organizativa.
- Presenta múltiples desafíos técnicos que van desde la celeridad en los tiempos de respuesta del sistema en su conjunto, al tratamiento de una población con limitaciones naturales frente a las tecnologías digitales en general y en particular a las biométricas en razón de su franja etaria.

A partir de los argumentos expresados, dentro del presente capítulo se introduce al sistema Mi Huella por medio de una descripción general del mismo. En segundo término, se lleva a cabo una revisión analítica de la información obtenida sobre el caso, con la finalidad específica de alcanzar:

- Un compilado de normas de aplicación específica sobre el sistema.

[7] Ref. Bibliográfica [7] https://www.anses.gob.ar/informacion/datos-abiertos-pasivos Descarga formato XLSX P.2.1 - Total País. Titulares únicos con al menos una jubilación o pensión contributiva. Casos y haberes medios.

- Una valoración de los aspectos normativos de Mi Huella en cuanto a la protección de los datos biométricos en general y en particular en el almacenamiento y conservación, tanto en sí mismos como en forma comparativa a los del marco general.
- Una revisión de las tecnologías aplicadas para el almacenamiento de datos biométricos.

3.2. Sistema de Identificación Biométrica de ANSES SBA o Mi Huella

SBA es una aplicación encarada actualmente como un servicio web que permite reconocer la identidad de las personas a través de la digitalización de sus huellas dactilares. El sistema se utiliza fundamentalmente a propósito de lo que se llama prueba de supervivencia o fe de vida de los beneficiarios de jubilaciones y pensiones, con el objeto de garantizar que los haberes previsionales sean percibidos sólo por ellos (o por sus apoderados legales). Al estar automatizados los pagos a través de cajeros electrónicos, ocurría que el titular del beneficio fallecía y otra persona en poder de su tarjeta bancaria y de su clave continuaba cobrando los haberes hasta mucho tiempo después.

Figura 3 Información sobre Mi Huella en sitio web de ANSES

Técnicamente, el sistema SBA valida la identidad de las personas por medio de terminales instaladas en las entidades bancarias que operan con el ANSES y que hacen uso de la infraestructura propia de este organismo. Las operaciones biométricas que se realizan son, básicamente, la de carga de datos (enrolamiento) y la de verificación de identidad.

Para la operatoria referida, el SBA cuenta con un servicio web que implementa una arquitectura SOAP de transacciones sincrónicas y asincrónicas, cada una de las cuales está identificada por un identificador único. SOAP (la sigla significa originariamente Simple Object Access Protocol) es un protocolo estándar que permite que dos objetos en diferentes procesos puedan comunicarse por medio de intercambio de datos XML. Se trata de uno de los protocolos más utilizados en los servicios web.

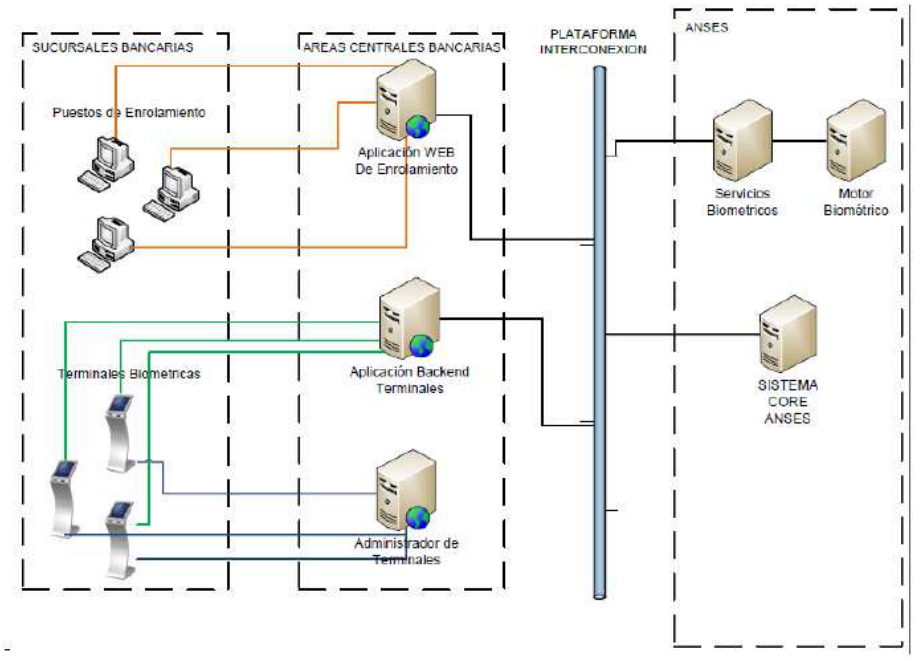


Figura 4 Esquema de partes intervinientes en SBA. Fuente Anexo II Res. 57 ANSES

Como se aprecia en la figura anterior, tres son las partes principales que intervienen en el sistema:

- Las sucursales bancarias con sus puestos de enrolamiento y sus terminales biométricas.
- Las áreas centrales bancarias con sus aplicaciones centralizadas que interactúan a través de la plataforma de interconexión con ANSES.
- La ANSES con sus sistemas centrales y sus servicios biométricos conectados a un motor (base de datos) biométrico.

Figura 5 Trámite de enrolamiento esquematizado en sitio web de ANSES

3.3. Marco normativo específico de Mi Huella o SBA

Seguidamente se incluye una compilación de las normas que forman el marco reglamentario de Mi Huella en relación con la protección de datos personales. Naturalmente, este marco específico está circunscripto al general, que fuera analizado en el capítulo respectivo.

Ítem	Norma	Objeto y principales contenidos
1	Resolución D.E.-N N° 567 de 30 de diciembre de 2013	Aprobó el "NUEVO RÉGIMEN INTEGRADO PARA EL PAGO DE PRESTACIONES DE LA SEGURIDAD SOCIAL" y dispuso que las entidades pagadoras deberán incorporar herramientas biométricas de identificación en cada una de sus Sucursales, Centros de Pago y Mini Centros de Pago en las que se efectúe el pago de prestaciones correspondientes a jubilaciones y pensiones del SISTEMA INTEGRADO PREVISIONAL ARGENTINO (SIPA) y pensiones no contributivas.
2	Resolución ANSES 648 / 2014	Complementa y amplía lo dispuesto en el Régimen establecido por la Resolución D.E.-N N° 567/13, a fin de incorporar el uso de herramientas biométricas de identificación por huella digital. Aprueba las pautas básicas del funcionamiento del Sistema de Identificación Biométrica ANSES, SBA, modifica lo aprobado por Resolución DE N N°567/13 y en particular aprueba como ANEXO II las condiciones funcionales, técnicas y el procedimiento referido al Sistema de Identificación Biométrica en reemplazo del ANEXO II aprobado por la Resolución DE-N N° 567/13; como ANEXO

Ítem	Norma	Objeto y principales contenidos
		III los Diseños de Registro en reemplazo del ANEXO III aprobado por la Resolución DE-N N° 567/13 y como ANEXO IV el modelo de Convenio de Pago de Prestaciones de la Seguridad Social en reemplazo del ANEXO IV aprobado por la Resolución D.E.-N N° 567/13.
3	Resolución ANSES Subdirección Ejecutiva de Administración 57-E/2017	Aprueba el ANEXO II de la Resolución D.E.-N Nº 648/14, el cual quedará redactado según se detalla en el ANEXO N° IF-2017-02690249-ANSES-DGIEIT#ANSES de la presente Resolución.
4	ANEXO II N° IF-2017-02690249-ANSES-DGIEIT#ANSES	Es una guía de procedimientos que propone definiciones, componentes del sistema de identificación biométrica, puestos de enrolamiento, aplicación de enrolamiento, consideraciones sobre la seguridad, lector biométrico, características y certificaciones del lector biométrico, tótem biométrico y sus requerimientos mínimos, aplicación tótem biométrico, servicio beneficiarios, archivo actualización de datos del beneficiario e informe supervivencia, contingencia, plataforma de interconexión, secuencia de pasos para acceso a los servicios, pautas y protocolos de identificación, autenticación y autorización, especificaciones de los servicios, estructuras de datos y descripción de los métodos, principales errores genéricos, requerimientos y especificaciones técnicas para los enlaces de datos y base biométrica.

Tabla 2 Marco normativo específico del SBA. Elaboración propia.

De las normas que sirven de marco específico al SBA, enunciadas y explicadas sucintamente en la tabla anterior, las de mayor relevancia en el terreno práctico son, sin dudarlo, las dos resoluciones de ANSES que instrumentan y actualizan en forma sucesiva el llamado Anexo II, el cual resulta en la práctica una guía del procedimiento a seguir en todos los aspectos vinculados a la operatoria del sistema en su conjunto y a cada parte responsable.

La Resolución de ANSES N° 648 del 2014 extiende el sistema de acreditación de la fe de vida a través de la identificación por huella dactilar a un universo de beneficiarios más amplio (todos los titulares o apoderados de jubilaciones y pensiones del SIPA y de pensiones no contributivas) y obliga a las entidades bancarias a incorporar en cada una de sus sucursales y centros de pagos en los que se realizaran pagos de beneficios correspondientes a jubilaciones y pensiones del SIPA (Sistema Integrado Previsional Argentino) un

Sistema de Control Biométrico de acuerdo a las especificaciones técnicas detalladas en el Anexo II, previa suscripción del convenio modelo aprobado por el Anexo IV de la misma resolución.

También dicha resolución determina que el responsable de realizar el enrolamiento del beneficiario tiene la obligación de acreditar fielmente la identidad de la persona que registra su huella dactilar en el Sistema de Identificación Biométrica, requiriéndole la documentación de respaldo legal que acredite la misma (DNI, libreta cívica o de enrolamiento militar).

La norma indica que en cada entidad pagadora se debe realizar únicamente el enrolamiento de los titulares que perciban las prestaciones en dicha entidad. Por fin, los beneficiarios que deban darse de alta en el Sistema de Control Biométrico con posterioridad a la fecha de finalización del plazo de implementación del referido sistema serán enrolados por ANSES, situación que acontece al momento del presente análisis. Es decir, ANSES lleva adelante el enrolamiento de los nuevos beneficiarios o sus apoderados, directamente en sus dependencias, no obstante, todavía se da el enrolamiento en las entidades bancarias.

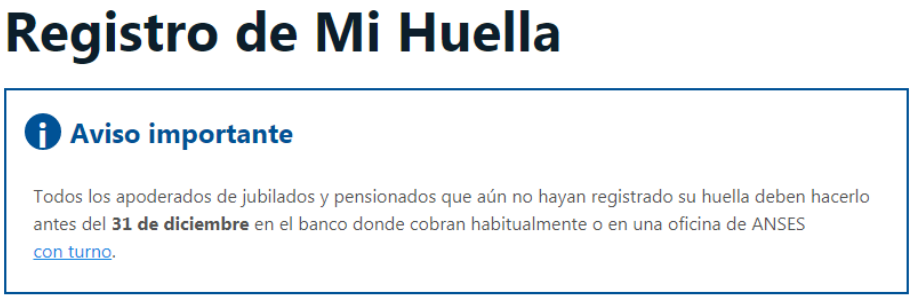


Figura 6 Aviso en sitio oficial de ANSES sobre lugares y plazos de enrolamiento.

La resolución también señala que los datos biométricos recolectados por ANSES serán resguardados en una única Base de Datos de Registros Biométricos que será administrada por la Dirección General Diseño de Normas y Procesos.

Indica además, que para el supuesto de que se produzca algún inconveniente técnico que imposibilite la conexión con los sistemas, se detecten inconsistencias durante el proceso de enrolamiento o de verificación de datos de

huellas dactilares, las entidades bancarias deben garantizar el pago de las prestaciones previsionales a los beneficiarios y/o apoderados en su cápita.

Por último, la resolución aprueba los diferentes anexos reemplazantes de los establecidos por la Resolución DE-N N° 567/13, a la vez que faculta a la Subdirección Ejecutiva de Administración a establecer, modificar y adecuar los diseños de registro aprobados en la presente resolución y a dictar las normas complementarias y reglamentarias que considere necesarias para la implementación del presente sistema. Los anexos referidos son el Anexo II de condiciones funcionales, técnicas y el procedimiento referido al Sistema de Identificación Biométrica, el Anexo III de diseños de registros y el Anexo IV de modelo de Convenio de Pago de Prestaciones.

Es precisamente la facultad señalada en el párrafo anterior, la que permite a la referida Subsecretaría dictar la Resolución N° 57 del 2017 por la que nuevamente se reemplaza el Anexo II, es decir el conjunto de condiciones funcionales, técnicas y de procedimiento referidas al SBA. Cabe destacar que el reemplazo es más que nada una actualización técnica con mayor grado de detalle y de precisión en varios aspectos.

Cabe aclarar que las características del SBA que se describirán en el apartado siguiente, se corresponden con la última versión del Anexo II.

3.4. Características técnicas, de calidad y de seguridad del SBA

Las especificaciones del servicio SBA señalan que cada entidad bancaria que desee operar sus sistemas con el SBA deberá implementar cuatro funcionalidades, a saber:

- Consulta del estado de un CUIL (Método GetCuilState).
- Carga de datos o enrolamiento (Método Enroll).
- Consulta del estado de la transacción de enrolamiento (Método GetEnrollResult).
- Verificación de Identidad (Método Verify)

En particular, la aplicación de enrolamiento de la entidad bancaria, que es la que captura y registra de algún modo las huellas dactilares, permite, en un primer paso, el ingreso del CUIL (Clave Única de Identificación Laboral) de la

persona a enrolar (cuya identidad será previamente verificada con alguna identificación personal exhibida, tal como documento nacional de identidad o DNI). Luego, ese CUIL se utiliza para indagar el estado de la persona ante el SBA (básicamente, por enrolar o ya enrolado). Si como resultado de la consulta le corresponde enrolar a la entidad bancaria, el aplicativo facilita la captura de 4 huellas dactilares, con un orden y prioridad preestablecidos, de conformidad con las condiciones naturales o reales de los dedos de las personas (falanges y yemas existentes, huellas legibles) Una vez capturadas las huellas, el aplicativo debe enviar el CUIL y las huellas capturadas, en principio cuatro (dos dedos índices y dos dedos pulgares) al SBA.

3.4.1. Datos de entrada para el método enrolamiento (Enroll)

En relación con los datos provenientes del enrolamiento, destinados a ser almacenados en la base centralizada de ANSES, se especifican los siguientes como parámetros de entrada:

Nombre	Descripción
Document	Documento del beneficiario, estructura **Document** según se detalla en el ítem **12.5.** Este método solo acepta tipo CUIL.
Fingers	Arreglo de huellas, arreglo de estructuras **Finger**, se detalla en el ítem **12.6.** Las 4 huellas capturadas deben ser enviadas con su identificación de dedo y se envía el WSQ encriptado. No se envía Template.
Entity	CUIT de la entidad bancaria
Terminal	Código que identifica una terminal de la entidad
Metadata	Arreglo de pares de valores (Name, Value). Se usan para enviar los datos de contacto. Como se especifica en la siguiente tabla.

Figura 7 Estructura DATOS entrada para ENROLAMIENTO. Fuente: Anexo II Res. 57

Para conocer algo más del diseño de los registros de entrada y (posiblemente) de los de almacenamiento, se agregan las estructuras Document y Finger mencionadas en la tabla de la figura anterior.

12.5 Estructura Document

Nombre	Descripción
DocumentNum	Número de documento. (solo números, sin espacios, puntos o guiones) Ej.: DNI = 42654480 CUIL = 20426544807 Argenta = 5370767200001650
Nationality	Nacionalidad documento con codificación de países según norma ISO 3166-1 alfa-3. Actualmente solo puede tomar el valor "**ARG**".
TypeId	Tipo de documento. Los valores que puede tomar se describen son "**CUIL**", "**DNI**", "**AR**" (Tarjeta Argenta)

12.6 Estructura Finger

Nombre	Descripción
FingerType	Tipo de dedo. Los valores que puede tomar se describen en 12.6.1
FingerprintType	Tipo de huella. Se usará siempre LiveScanPlain
IsAmputation	Indica amputación dedo (true ó false)
Template	Minucia de 1Kb de tamaño promedio.
TemplateFormat	Formato Minucia. Los valores que puede tomar se describen en 12.6.3
WSQ	Imagen WSQ (sólo en enrolamiento) firmado y encriptado mediante PKCS#7 (*). Tamaño promedio de 20Kb

Figura 8 Estructura DOCUMENT y FINGER. Fuente: Anexo II Res. 57

El asterisco (*) en el último campo WSQ define que la captura de cada huella dactilar debe ser transmitida encriptada según el estándar PKCS#7, firmando el archivo wsq con el certificado de la entidad bancaria y encriptando con el certificado público de ANSES. Ambos certificados son provistos por la ANSES. Cabe señalar que al momento de la elaboración del presente, el certificado de ANSES como Autoridad Certificante lleva algún tiempo de expirado y sin novedades en cuanto a que estén en trámite de renovación.

Además se especifica que el formato de minucias debe corresponderse con la norma ANSI1378, mientras que adicional y optativamente se puede agregar el formato Neurotechnology.

Seguidamente, la estructura de los metadatos del enrolamiento.

Name	Value
Calle	Domicilio del beneficiario/apoderado (Obligatorio)
Numero	Número (Obligatorio)
Piso	Piso
Depto	Identificación si fuera departamento
Anexo	Anexo
Torre	Torre
Sector	Sector
Manzana	Manzana
Pais	País (Obligatorio)
Provincia	Provincia (Obligatorio)
Localidad	Localidad (Obligatorio)
CP	Código Postal Numérico (Obligatorio)
CPAlfa	Código Postal Alfanumérico
Telefono	Número de teléfono de contacto del beneficiario (Obligatorio)
TipoTelefono	Fijo/Celular (Obligatorio)
CorreoElectronico	Correo Electrónico de contacto del beneficiario

Figura 9 Estructura METADATOS para ENROLAMIENTO. Fuente: Anexo II Res. 57

3.4.2. Datos de entrada para el método de verificación (Verify)

Los parámetros de entrada para el método de verificación de identidad, el cual es en definitiva el corazón del servicio Mi Huella, son los expresados en la siguiente tabla y como se verá, resultan similares a los previstos en la instancia de enrolamiento.

Nombre	Descripción
Document	Documento del beneficiario, estructura **Document** según se detalla en el ítem **12.5.**
Fingers	Arreglo de huellas, arreglo de estructuras **Finger**, se detalla en el ítem **12.6.** El parámetro FingerType debe ser **Unknown,**
Entity	CUIT de la entidad bancaria
Terminal	Código que identifica una terminal de la entidad
Metadata	Arreglo de pares de valores (Name, Value) Se usan para enviar los datos del dispositivo con el que se captura la huella.

Figura 10 Estructura DATOS VERIFICACIÓN. Fuente Anexo II de Res. 57

3.4.3. Mecanismos de comunicación y de calidad previstos

Durante todo el tiempo respectivo a la implementación del sistema y sobre todo en el período correspondiente al mecanismo de enrolamiento distribuido entre las diferentes entidades bancarias, se dispuso que, desde el momento de la captura hasta el envío de datos biométricos a ANSES, bajo un enlace encriptado

mediante SSL, cada banco debía establecer los mecanismos de protección de la imagen para evitar su pérdida o alteración, y mantener su confidencialidad.

Con ese objetivo se estableció que los mecanismos de encriptación debían garantizar que la información capturada se encontrara segura hasta el momento de la transmisión, lo cual implica que se previeron de manera implícita, desde el momento de la captura inicial, instancias de acopio y almacenamiento de datos biométricos en las entidades bancarias, sin que se establecieran mayores imperativos respecto de su vaciamiento o eliminación una vez transmitidos esos datos biométricos a la base de datos centralizada.

Asimismo, en el marco de la implementación del SBA, se tomaron previsiones respecto del mecanismo de captura (Escáner Multiespectral) y del formato de imágenes a enviar (WSQ), cuestiones éstas que impactan en la mayor o menor nitidez de las imágenes, aspecto directamente asociado al nivel de desempeño de los procesos de lectura de las mismas.

Otra cuestión normada, también vinculada a la calidad de las imágenes y por ende a la seguridad del sistema, refiere a que el sensor de huellas digitales debe incluir tecnología de imágenes multiespectral, a los efectos de permitir la lectura de huellas en condiciones deterioradas, con cierta suciedad, envejecidas, secas o húmedas. Dicha tecnología debe respetar los siguientes parámetros:

- Conexión mediante USB 2.0 Alimentación eléctrica mediante el mismo conector USB.
- Soporte para Sistemas Operativos Microsoft Windows /Linux (32-bits y 64-bits)
- Resolución de 500 dpi, 8-bits de profundidad, escala de grises 256.
- Tipo de sensor óptico con iluminación Multi-espectral
- Protección de latentes
- Captura por contacto
- Detección de dedo vivo por software/hardware, actualizable
- Protección IP65 para la platina
- Opcional: soporte criptográfico 3DES

Un aspecto que se debe resaltar es que queda a criterio de la entidad bancaria la encriptación en el lector biométrico. Es decir, que no se previeron parámetros o requisitos a cumplir para esta cuestión desde la reglamentación de ANSES.

En relación con la calidad de las imágenes de huellas dactilares, el National Institute of Standars and Technology (NIST) creó oportunamente un sistema de categorización denominado NIST Fingerprint Image Quality (NFIQ). El NFIQ de una huella es un valor comprendido entre 1 y 5 que indica cuál es la probabilidad de detectar un error debido a la calidad de sus minucias (características de las crestas y valles de los surcos de cada huella). A partir del año 2011, el Instituto comenzó una revisión integral del algoritmo NFIQ y ya es posible hablar de una versión NFIQ 2.0. [8]

Conforme lo define el Anexo II de la Resolución 57 del 2017, el valor de NFIQ es una predicción del rendimiento del motor de búsqueda; que refleja la contribución positiva o negativa de una muestra individual con el rendimiento global de un sistema de comparación de huellas dactilares.

Los cinco niveles de calidad de NFIQ suelen ser predictivos del nivel de desempeño de un sistema de búsqueda a través de minucias de la huella dactilar, de acuerdo a los extremos de la siguiente escala:

NFIQ = 1 indica una buena calidad de muestra.

NFIQ = 5 indica una mala calidad de muestra.

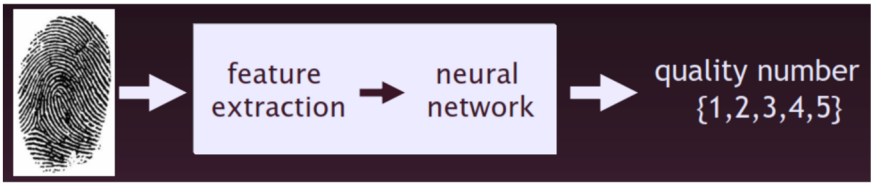


Figura 11 Esquema simple del algoritmo NFIQ. Fuente: Anexo II Resolución 57

La figura anterior muestra esquemáticamente cómo se llega de lectura de la imagen al número indicativo del NFIQ. Para ello describe los siguientes elementos:

- Feature extraction (Extracción de características): Extracción de las características (minucias) de la imagen, generando un vector de 11 dimensiones con dichas características.

[8] Referencia bibliográfica [8] Página oficial de NIST https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis.

- Neural network (Red neuronal): Clasifica el vector de características en cinco clases de calidad basándose en varias calidades de la distribución normal del valor de coincidencia.

Tal como ya se indicó, el índice de calidad es un valor entero entre 1 (Mejor calidad) y 5 (Peor calidad), mientras que la calidad mínima aceptada por el SBA es igual a 3. También se indica que para calidades 4 o 5 se deberán realizar hasta 3 reintentos de captura. De no ser posible obtener una mejor calidad será necesario capturar la imagen de huella de otros dedos hasta completar las cuatro huellas requeridas por SBA.

Con el propósito de establecer las principales características de la última versión de NFIQ, cabe señalar que NFIQ 2.0 [9]:

- Está desarrollado para imágenes capturadas a 500 ppp y, como tal, no debe usarse para imágenes de diferente resolución.
- Está desarrollado para imágenes capturadas con sensores ópticos o escaneadas desde una tarjeta entintada.
- NFIQ 2.0 emplea el extractor de minucias FingerJet FX OSE, que es un extractor de minucias de código abierto bajo los términos de una licencia pública de la Free Software Foundation.
- Además, NFIQ 2.0 utiliza una implementación OpenCV de árboles aleatorios (Forest / tree random). Un algoritmo orientado a resolver de manera eficiente los problemas de clasificación y de regresión que se dan típicamente al momento de comparar imágenes.

Cabe destacar que no se ha podido verificar cuál es la versión de NFIQ actualmente utilizada en el SBA.

La reglamentación del SBA señala que será la propia ANSES quien comunicará a las entidades bancarias cuáles son los lectores biométricos homologados para la verificación de fe de vida. Además, determina que cada entidad podrá requerir la homologación de un lector biométrico no incluido entre los homologados por ANSES en cualquier momento del ciclo de vida del proyecto. Ante esa solicitud, ANSES podrá homologar el lector ya sea por intervención de sus áreas técnicas o mediante consulta a entidades técnicas externas con conocimientos específicos en la materia.

Las aplicaciones de enrolamiento y las aplicaciones del tótem del servicio del SBA deben hacer uso de la plataforma de interconexión de ANSES. Se

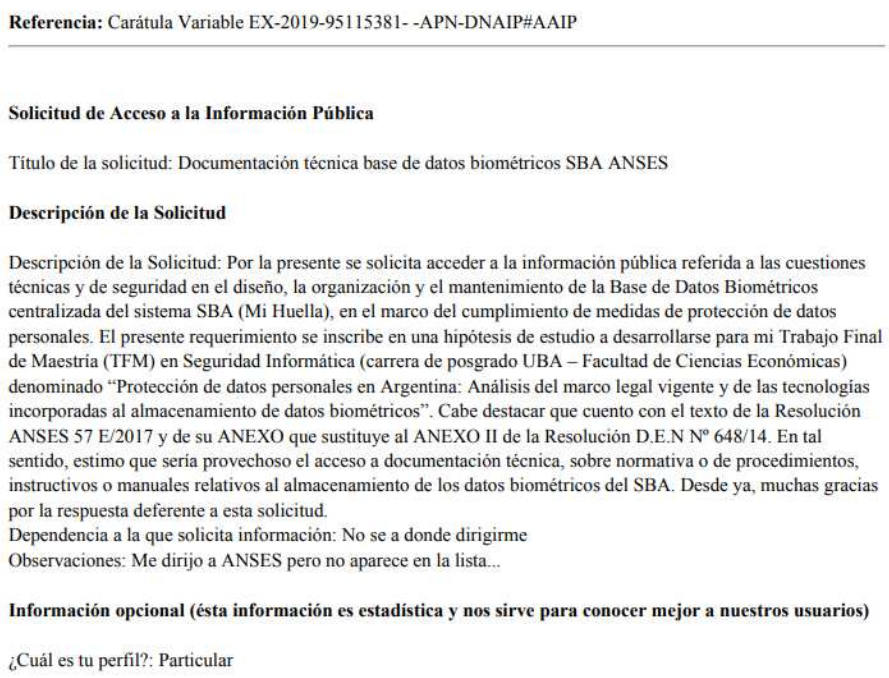
[9] Ref. Bibliográfica [9] https://www.nist.gov/services-resources/software/development-nfiq-20.

detallan a continuación los estándares a utilizar en la implementación de un cliente (o consumidor) estándar del servicio SBA a través de la plataforma:

- HTTP como protocolo de transporte de alto nivel
- SSL como seguridad en la capa de transporte
- SOAP versión 1.1 /1.2 como protocolo de mensajería
- XML versión 1.1 como formato de representación
- WSDL versión 1.1 como lenguaje de descripción de servicios
- CMS (PKCS#7) versión 1.5 para firma de mensajes
- PKCS#10 versión 1.7 como estándar de solicitud de certificado

3.5. El pedido de información acerca de Mi Huella

El día 22/10/2019 se presentó un pedido de acceso a la información pública a través de la plataforma de tramitación a distancia (TAD) del sitio argentina.gob.ar. Para ello se inició el expediente código EX-2019-95115381-APN-DNAIP#AAIP a los efectos de gestionar la solicitud de información técnica y de cuestiones relativas a la seguridad de los datos biométricos almacenados en el sistema Mi Huella, aclarándose todo lo posible el alcance y el propósito del pedido.



Referencia: Carátula Variable EX-2019-95115381- -APN-DNAIP#AAIP

Solicitud de Acceso a la Información Pública

Título de la solicitud: Documentación técnica base de datos biométricos SBA ANSES

Descripción de la Solicitud

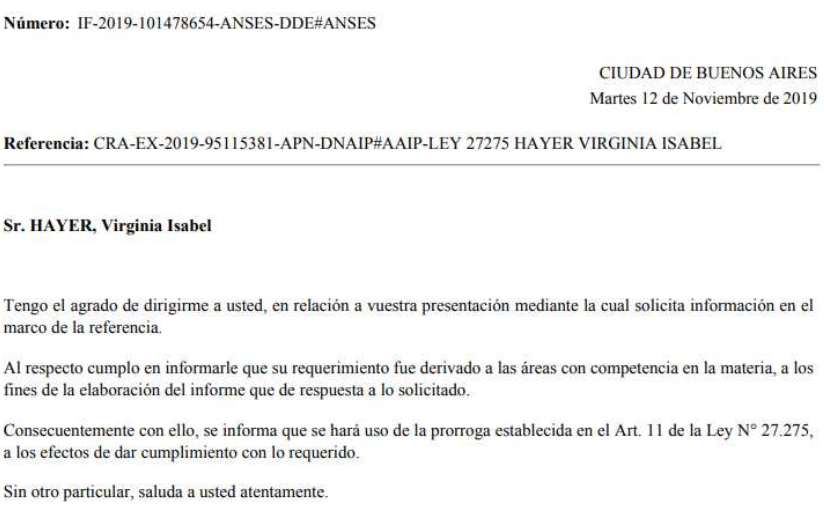
Descripción de la Solicitud: Por la presente se solicita acceder a la información pública referida a las cuestiones técnicas y de seguridad en el diseño, la organización y el mantenimiento de la Base de Datos Biométricos centralizada del sistema SBA (Mi Huella), en el marco del cumplimiento de medidas de protección de datos personales. El presente requerimiento se inscribe en una hipótesis de estudio a desarrollarse para mi Trabajo Final de Maestría (TFM) en Seguridad Informática (carrera de posgrado UBA – Facultad de Ciencias Económicas) denominado "Protección de datos personales en Argentina: Análisis del marco legal vigente y de las tecnologías incorporadas al almacenamiento de datos biométricos". Cabe destacar que cuento con el texto de la Resolución ANSES 57 E/2017 y de su ANEXO que sustituye al ANEXO II de la Resolución D.E.N Nº 648/14. En tal sentido, estimo que sería provechoso el acceso a documentación técnica, sobre normativa o de procedimientos, instructivos o manuales relativos al almacenamiento de los datos biométricos del SBA. Desde ya, muchas gracias por la respuesta deferente a esta solicitud.
Dependencia a la que solicita información: No se a donde dirigirme
Observaciones: Me dirijo a ANSES pero no aparece en la lista...

Información opcional (ésta información es estadística y nos sirve para conocer mejor a nuestros usuarios)

¿Cuál es tu perfil?: Particular

Figura 12 Copia del pedido de acceso a la información pública sobre Mi Huella

Con fecha 13/11/2019 fue notificado a la casilla de correo (identificada como domicilio electrónico de la usuaria de la plataforma TAD), un aviso de prórroga en los términos del artículo 11 de la Ley N° 27.275, lo cual implica un paréntesis de un máximo de 15 días hábiles, a contar desde la fecha antedicha.



Número: IF-2019-101478654-ANSES-DDE#ANSES

CIUDAD DE BUENOS AIRES
Martes 12 de Noviembre de 2019

Referencia: CRA-EX-2019-95115381-APN-DNAIP#AAIP-LEY 27275 HAYER VIRGINIA ISABEL

Sr. HAYER, Virginia Isabel

Tengo el agrado de dirigirme a usted, en relación a vuestra presentación mediante la cual solicita información en el marco de la referencia.

Al respecto cumplo en informarle que su requerimiento fue derivado a las áreas con competencia en la materia, a los fines de la elaboración del informe que de respuesta a lo solicitado.

Consecuentemente con ello, se informa que se hará uso de la prorroga establecida en el Art. 11 de la Ley N° 27.275, a los efectos de dar cumplimiento con lo requerido.

Sin otro particular, saluda a usted atentamente.

Figura 13 - Copia del pedido de prórroga notificado

En el día del vencimiento de la prórroga, 6/12/2019, se notifica la respuesta producida por ANSES por medio de la nota NO-2019-101457750-ANSES-DS#ANSES y su documento adjunto. Se trata de una información muy escueta, la cual se agrega en forma completa como ANEXO al presente capítulo, pudiendo resumirse como sigue:

- Se señala que las huellas se guardan en formato WSQ (imágenes) en SIA (presumiblemente Sistema de Información de ANSES, orientado a los beneficiarios de la seguridad social que integra el SBA o lo comprende) y los modelos representativos de las huellas (las minucias) en los motores de Megamatcher.
- Además se agregan los modelos de datos de las bases SIA y SBA.

A los efectos del presente estudio, la información suministrada por ANSES permite tratar de manera indiferenciada o como un conjunto al SIA y al SBA, verificar el modelo de datos en su conjunto y conocer cuáles son algunas de las tecnologías utilizadas, por ejemplo, la llamada Megamatcher, cuyo estudio con mayor grado de detalle se verá en el capítulo respectivo.

Sin embargo, pese al pedido expreso al respecto, lo respondido por ANSES no hace ninguna referencia directa a los cuidados o las medidas de seguridad diseñadas o implementadas en el almacenamiento de los datos biométricos, por lo que podría inferirse que los que existan sólo serán los suministrados por el propio modelo de datos o a través de los estándares de la tecnología Megamatcher utilizada.

Para concluir el presente capítulo, en el siguiente apartado se hará una valoración en general de los aspectos de seguridad analizados sobre el SBA y en particular, en relación con el almacenamiento de los datos biométricos.

3.6. Condiciones de seguridad en general y del almacenamiento en particular

En primer término y en relación con la seguridad en las comunicaciones, cabe señalar que está previsto que las aplicaciones de enrolamiento y las del tótem del Servicio del Sistema Biométrico ANSES (SBA), mayormente dedicadas a la verificación de la identidad, hagan uso de la plataforma de interconexión de ANSES, la cual se encuentra conformada por un sistema de autenticación y un sistema de autorización que permiten ejecutar las acciones del servicio SBA dentro de un nivel de seguridad aceptable, alineado con el estándar actual del mercado.

Además, entre otros aspectos de seguridad para la transmisión de imágenes de huellas, se había previsto que éstas se enviaran encriptadas durante el proceso de enrolamiento en las sedes de las entidades bancarias. Al momento actual, en el que el enrolamiento también puede realizarse directamente en oficinas de ANSES, se desconoce si la previsión del encriptado prevalece también en los casos de comunicación entre oficinas de atención al público de ANSES y su sede central.

También cabe resaltar que lo previsto en torno a la encriptación de imágenes no se aplicaría necesariamente al caso de envío de imágenes de huellas capturadas durante el proceso de verificación o fe de vida. Ante esta situación, cabe preguntarse si los riesgos de seguridad durante la transmisión son diferentes cuando una imagen viaja para su cotejo, de cuando lo hace para ser almacenada.

Respecto de la seguridad en la captura y en la transmisión en sí de los datos biométricos, se debe destacar el protocolo de calidad NFIQ seleccionado, que estaría actualizado a las versiones más recientes del NIST (o estaría en camino de serlo). En este sentido, se destaca la exigencia de una calidad de nivel 1 o 2, siendo estos los más elevados, mientras que en el caso de que se capturen huellas con menor calidad, se deberán realizar hasta tres reintentos de captura y eventualmente, capturar la imagen de huella de otros dedos hasta completar las cuatro imágenes requeridas por el SBA. La calidad de la imagen está intrínsecamente asociada a la efectividad (menor cantidad de errores en el proceso de lectura, selección y comparación) y a la eficiencia en los tiempos de los procesos.

En relación con el almacenamiento de los datos biométricos, es dable señalar las siguientes condiciones y circunstancias que afectan o podrían afectar su seguridad. A saber:

Como procedimiento de contingencia, la normativa señala que en caso de que no se pueda realizar la invocación al servicio SBA en línea por cualquier motivo, se almacenarán temporalmente las huellas capturadas y se utilizará un proceso batch (por lote de transacciones) para realizar la transferencia de la información, utilizando los mismos métodos usados en el caso de realizar el enrolamiento o la verificación en línea.

También está previsto en la última versión del Anexo II que a requerimiento de una entidad bancaria, ANSES podrá proveer una copia de las minucias de las huellas de los beneficiarios enrolados en dicha entidad.

Si se agrega a las dos situaciones anteriores que no hay ningún tipo de norma de procedimiento, guía o protocolo que indique qué hacer con los datos biométricos capturados una vez transmitidos a la base centralizada de ANSES, es posible concluir que dicha base coexiste con múltiples bases parciales de datos biométricos de los beneficiarios en cada entidad bancaria que están en su cápita.

Por otra parte, refuerza este concepto de coexistencia de bases, el imperativo de que las entidades deben estar preparadas para dar respuesta a los beneficiarios a los que pagan, aún en caso de inconexión o salidas de servicio de la plataforma de ANSES.

Cabe la duda de cómo están almacenados los datos biométricos, más allá de los estándares de las minucias o de la calidad de las huellas y en el sentido de si se practican reglas de disociación de la información. En otras palabras, los datos de identidad, tipo y número de documento, nombre y apellido, CUIL, ¿se almacenan junto o contiguos a los biométricos? La misma pregunta cabe hacerse respecto de los metadatos que no son otra cosa que el domicilio completo del beneficiario y su dirección de correo electrónico.

Entonces, dos son las situaciones de riesgo a destacar vinculadas al almacenamiento. La primera y principal, que los datos estén insuficientemente disociados y que una intrusión o acceso indebido a la base de datos pueda provocar un estrago masivo y mayúsculo al revelar la identidad de los datos biométricos de millones de personas. La segunda, de menor alcance e impacto, pero quizás más probable, que cualquiera de esas bases parciales o muchas de ellas puedan estar en riesgo por el mismo motivo, disminuyendo por razones obvias la cantidad de casos afectados, pero multiplicadas, de la misma manera, las ocasiones de fallo por la cantidad de bases distribuidas.

Las conclusiones respecto de los estándares de seguridad implicados en la tecnología Megamatcher, se apreciarán en el capítulo respectivo al estudio de las tecnologías disponibles y utilizadas, así como en el propio de conclusiones en general.

Capítulo ESTUDIO DE LAS TECNOLOGÍAS DISPONIBLES Y UTILIZADAS

4.1. Introducción a los sistemas automatizados de huellas dactilares

Los sistemas automatizados de huellas dactilares se basan necesariamente en datos extraídos de imágenes y existe un sinnúmero de formas en los que una huella dactilar puede ser escaneada. Asimismo, el éxito en la identificación de huellas dactilares depende de la claridad de la imagen y del grado de coincidencia entre la huella origen de la búsqueda y la impresión o el registro en la base de datos comparado. Por otra parte, para completar este panorama inicial, debe señalarse que los algoritmos de representación, de normalización y de compresión de los datos, son los factores que usualmente inciden en la precisión de todo este proceso.

Figura 14 Ilustración de huella digital y sus minucias.

La tecnología de huella dactilar ha recorrido un largo camino desde sus inicios, hace más de 100 años. Los primeros lectores de huellas en vivo, introducidos a fines del siglo XX, eran aparatos de grandes dimensiones, llenos de complejidades y difíciles de manejar en comparación con los sencillos, baratos y relativamente minúsculos sensores disponibles en la actualidad.

Durante las últimas décadas, la investigación y el uso activo de comparación de huellas dactilares también han provocado avances en nuestra comprensión de la individualidad, la información de las huellas dactilares y las formas eficientes de procesar esta información. El abaratamiento de los equipos

de computación y de los sensores, aunado a una demanda cada vez más creciente de seguridad y eficiencia en la comprobación de identidades, han llevado al uso diario en múltiples aplicaciones de sistemas automáticos de huellas dactilares, es decir de sistemas llamados genéricamente AFIS (por la sigla en inglés respectiva). [10]

Se han desarrollado desde hace muchos años, múltiples modelos que comprueban la teoría de que no hay dos imágenes de crestas de fricción iguales, así como también para determinar la cantidad de minucias suficiente para establecer un nivel de calidad tal que permita la individualización con certeza. Sin embargo, todavía quedan algunos desafíos por superar, sobre todo en el diseño de un sistema de identificación de huellas dactilares totalmente automático y confiable, en especial cuando las imágenes de las huellas son de mala calidad.

Aun cuando no existen estándares universales para la calidad de la imagen de las huellas dactilares, el NIST (Instituto Nacional de Estándares y Tecnología de USA) ha desarrollado y publicado un software para medir la calidad de imagen de las huellas dactilares y es el que generalmente utilizan los proveedores de AFIS. El software se llama NIST Fingerprint Image Software.

4.2. Principales factores tecnológicos en los AFIS

Seguidamente, a los efectos de brindar un panorama más completo, se presenta un resumen de los principales aspectos tecnológicos a considerar en un AFIS:

4.2.1. Tecnologías para la adquisición de la imagen

Los datos de huellas dactilares se pueden recolectar mediante la aplicación de una fina capa de tinta sobre un dedo y el balanceo de ese dedo, de un lado a otro de la uña, presionando sobre una tarjeta de papel. Es lo que se hacía al principio y se denomina entintado de impresión.

Sin embargo, la transpiración y los contaminantes en la piel también resultan en la impresión de un dedo que se deposita sobre una superficie

[10] Ref. Bibliográfica [10] Kenneth R. Moses Autores colaboradores: Peter Higgins, Michael McCabe, Salil Prabhakar y Scott Swann CAPÍTULO 6 SISTEMA AUTOMATIZADO DE IDENTIFICACIÓN DE HUELLAS DACTILARES (AFIS) https://www.ncjrs.gov/pdffiles1/nij/250979.pdf sitio principal https://www.ncjrs.gov/ National Criminal Justice Reference Service.

determinada. Estas impresiones, que se denominan latentes, pueden ser química o físicamente reveladas, así como electrónicamente capturadas o manualmente levantadas desde la superficie mediante el uso de ciertas técnicas químicas, físicas y de iluminación, incluyendo su fotografía.

De tal manera, en principio, las impresiones de huellas dactilares se desarrollan y conservan usando cualquiera de los métodos anteriores, y pueden digitalizarse mediante el escaneo de la tarjeta de entintado, levantamiento o una fotografía. Las imágenes digitales adquiridas por este método se conocen como imágenes offline.

A partir de la década de 1970, los sensores de huellas dactilares comienzan a construirse para adquirir una imagen de la huella dactilar por escaneo en tiempo real o en vivo, directamente desde un dedo, sin el uso intermedio de tinta y una tarjeta de papel. Aunque las imágenes offline están todavía en uso en ciertas aplicaciones forenses y de gobierno, se utilizan cada vez más las imágenes de huellas dactilares escaneadas online.

Los principales parámetros que caracterizan una imagen de la huella dactilar son el área de resolución, el número de píxeles, la precisión geométrica, el contraste y la distorsión geométrica.

En la actualidad, la mayoría de los dispositivos de escaneo para aplicaciones comerciales suelen ser fáciles de utilizar, compactos y poco costosos. Hay una serie de mecanismos de detección ópticos, capacitivos, térmicos, basados en presión, ultrasonidos, o de otros tipos que pueden ser utilizados para detectar las crestas y valles presentes en la yema del dedo. Sin embargo, muchos de estos métodos no proporcionan imágenes que contengan la misma representación de detalles necesarios para algunas comparaciones de huellas dactilares latentes. Por ejemplo, una imagen capacitiva o térmica puede representar los bordes y poros de una manera muy diferente a una impresión de tinta.

Los dispositivos de escaneo suelen capturar una serie o un conjunto de imágenes de huellas dactilares a partir de una sola exploración. Dependiendo de la aplicación para la que el dispositivo fue diseñado, puede ejecutar uno o varios algoritmos. Por ejemplo, un algoritmo puede presentar en forma de mosaico con

múltiples imágenes adquiridas como un video durante una sola rodadura de un dedo sobre el escáner en una gran imagen laminada. Los algoritmos también suelen proporcionar vistas previas en tiempo real para ayudar al operador en la colocación o alineación correcta de los dedos.

Normalmente, un algoritmo de revisión de calidad de la imagen de una huella dactilar también se ejecuta para alertar al operador sobre la adquisición de una imagen de la huella con mala calidad, para que una de mejor calidad se pueda volver a adquirir del dedo. Aunque los escáneres ópticos tienen la historia más larga y la más alta calidad, los sensores de estado sólido comienzan a imponerse por su tamaño compacto y la facilidad con la que pueden ser incorporados en las computadoras portátiles, teléfonos celulares, bolígrafos inteligentes y similares.

Generalmente, para el proceso de captura de la imagen se utilizan los siguientes algoritmos:

- De captura automática de huellas dactilares.

  Inmediatamente después de que el sistema ha sido alertado de que un dedo está presente en la superficie del escáner, se inicia la recepción de una serie de imágenes y el algoritmo de captura automática de huellas dactilares determina qué fotograma de la secuencia de imágenes tiene la mejor calidad de imagen y elige esa toma del vídeo para su posterior tratamiento.

- Algoritmo de detección de vitalidad.

  El escáner puede determinar si el dedo es consistente con un ser humano vivo.

- Algoritmo de compresión de datos de imagen.

  La imagen comprimida requerirá menos capacidad de almacenamiento y de ancho de banda cuando se transfiera.

- Algoritmos de procesamiento de imágenes.

  Ciertas aplicaciones se benefician de la función de extracción llevada a cabo en el propio sensor; la transferencia de las características o minucias

de huellas dactilares también requerirá menos ancho de banda que la imagen.

- Algoritmo de emparejamiento de imagen y de protocolos criptográficos.

Ciertas aplicaciones implican que el emparejamiento de huellas dactilares se realice en el mismo sensor, por razones de seguridad, al igual que los necesarios para una comunicación segura.

4.2.2. Tecnologías para la extracción de características

Las singularidades de las crestas de huellas dactilares, comúnmente conocidas como puntos de minucia, se han utilizado tradicionalmente por los expertos forenses como las características clave para discriminar una huella de otra.

Las singularidades locales más comunes son las terminaciones de las crestas y las bifurcaciones de cada cresta. Otros tipos de minucias son simplemente compuestos de terminaciones de crestas y bifurcaciones. Por fin, las minucias formadas por dos a cuatro puntos característicos que se producen muy cerca unos de otros, también se han utilizado frecuentemente.

En un proceso tradicional y manual, un experto forense localizaría visualmente las minucias en una imagen de huella dactilar y señalaría su ubicación, la orientación de la cresta en la que reside y el tipo de minucias. Así, los algoritmos de extracción automática de características de las huellas dactilares fueron desarrollados para imitar la ubicación de las minucias realizada por expertos forenses.

Sin embargo, la mayoría de los algoritmos de extracción automática de minucias sólo considera las terminaciones de las crestas y las bifurcaciones porque otros tipos de detalles son muy difíciles de obtener automáticamente. Además, la mayoría de los algoritmos no diferencian entre las terminaciones de las crestas y las bifurcaciones, ya que pueden ser indistinguibles como resultado de las diferencias de presión del dedo durante la adquisición o por la aplicación del algoritmo de mejora.

Un enfoque común seguido por los algoritmos de extracción de características de huellas dactilares es utilizar primero un algoritmo de

binarización para convertir la imagen de la huella mejorada (escala de grises) a una forma binaria (blanco y negro) donde todos los píxeles negros corresponden a las crestas y los píxeles blancos corresponden a los valles. El algoritmo de binarización va desde un simple umbral de la imagen mejorada hasta algoritmos de localización de la cresta muy complejos.

Después de eso, un algoritmo de adelgazamiento se utiliza para convertir la imagen de la huella binaria en un único ancho de píxel sobre la línea central de la cresta. A la imagen resultante se la llama imagen adelgazada o imagen esquelética.

Por fin, un algoritmo de detección de minucias se aplica a esta imagen esquelética para localizar las coordenadas “x,y”, así como la orientación de los puntos de minucias. En la imagen esquelética, por definición, todos los píxeles en una cresta tienen dos píxeles vecinos en lo inmediato. Si un píxel tiene un solo píxel vecino, se determina que es una terminal de la cresta y si un pixel tiene tres píxeles vecinos, se determina que es una bifurcación de la cresta.

Cabe destacar que cada uno de los algoritmos utilizados en la mejora de imagen de la huella capturada y en la extracción de minucias tiene su propia limitación, proporcionando un procesamiento defectuoso, en particular por la detección de falsas minucias cuando la imagen original está demasiado sucia.

Para aliviar este inconveniente, se utiliza un algoritmo posterior que permite confirmar o validar las minucias detectadas. Sólo aquellas minucias que pasan este algoritmo de post procesado se guardan y el resto se elimina. Por ejemplo, si una longitud de la cresta que se extiende lejos del punto de minucias es suficiente o si la dirección de la cresta en el punto está dentro de los límites aceptables, las minucias se mantienen. Más adelante, la imagen puede ser invertida en escala de grises, convirtiendo el blanco al negro y el negro al blanco. El reprocesamiento de esta imagen invertida debe dar paso a las terminaciones de minucias en lugar de las bifurcaciones y viceversa.

Cabe destacar que las etapas y algoritmos descritos para la extracción de minucias representan solo el procedimiento más típico o usual. En la realidad, existe una amplia variedad de algoritmos que difieren unos de otros, tanto en sus componentes como en el orden en el que se aplican.

Muchas otras características pueden extraerse también aunadas a las minucias. Estas características adicionales a menudo proveen información útil que puede ser utilizada en las etapas de emparejamiento subsecuentes para mejorar la exactitud del emparejamiento de las huellas dactilares.

A su vez, recientemente han surgido algunos algoritmos automáticos de extracción (y emparejamiento) de características de huellas dactilares que utilizan información que no está basada en minucias de las imágenes de huellas dactilares. Por ejemplo, los poros sudoríparos, que son muy minuciosos en los de detalles de las huellas dactilares, más pequeños que los puntos de minucias, se han extraído con éxito por medio de imágenes de alta resolución.

4.2.3. Tecnologías para el emparejamiento

El emparejamiento de la huella dactilar puede definirse como el ejercicio de encontrar el grado de coincidencia entre dos imágenes de huellas dactilares dadas. También puede visualizarse al superponer una copia de papel de una imagen de huella dactilar almacenada, con sus minucias marcadas, con una transparencia de una huella dactilar de búsqueda, también con sus minucias marcadas.

Al colocar la transparencia de la impresión de búsqueda sobre la copia de papel de la huella dactilar de archivo y al trasladar y rotar la transparencia, se pueden localizar los puntos de minucias que son comunes en ambas impresiones. A partir del número de minucias comunes encontradas en el proceso, es posible evaluar la similitud de los dos puntos.

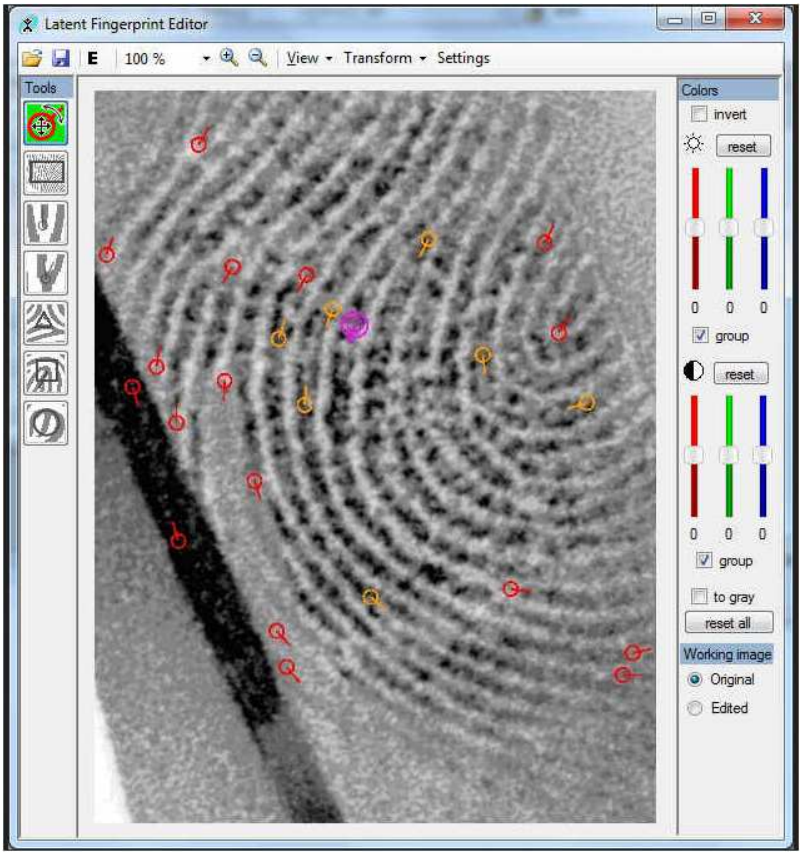


Figura 15 Editor de huellas latentes. Fuente: Ref. Bibliográfica [12]

Por supuesto, el emparejamiento manual de la huella dactilar es una tarea prácticamente imposible de emprender ante grandes volúmenes, de manera que se han ido desarrollando algoritmos que la automatizan.

El emparejamiento automático de una huella dactilar determinada puede realizar comparaciones a una velocidad de 30.000 veces por segundo o más y los resultados combinarse con cualquier otro criterio disponible para filtrar por fin a los candidatos.

Cabe destacar que las etapas y elementos descritos anteriormente representan solo un algoritmo típico de emparejamiento de minucias de la huella dactilar. Existen muchas variantes de este tipo y todas difieren entre sí. Al igual que los varios algoritmos de extracción, los de emparejamiento utilizan diferentes implementaciones, diferentes etapas y diferentes órdenes de etapas.

4.2.4. Tecnologías de indexación y recuperación

En el apartado anterior, se definió el emparejamiento como la acción de encontrar la similitud (o no) entre cualquier par de huellas dactilares dado. Hay

muchas situaciones, tales como el control de acceso físico dentro de una ubicación, por ejemplo, donde una sola coincidencia entre dos huellas dactilares bastará. Sin embargo, en la gran mayoría de las aplicaciones forenses y gubernamentales, tales como en las revisiones de antecedentes, se requiere que múltiples huellas dactilares (de hecho, más de 10 huellas dactilares de los 10 dedos de la misma persona) sean emparejadas contra un gran número de huellas dactilares presentes en una base de datos. En estas aplicaciones, se necesitará una gran cantidad de búsquedas de huellas dactilares y su respectivo emparejamiento para alcanzar una única identificación, lo cual consume mucho tiempo en principio.

Al igual que lo que ya se señaló en los factores anteriores, los algoritmos automáticos iniciales de indexación de la huella dactilar fueron desarrollados para imitar la labor de los peritos forenses. Así, inicialmente, se construyeron para clasificar las imágenes de huella dactilar en cinco clases típicas basadas en las características que pueden extraerse de forma automática.

Actualmente, la clasificación de patrones de huellas dactilares también puede determinarse mediante la aplicación de uno de los muchos posibles clasificadores generalizados, por ejemplo las redes neuronales, entrenados para reconocer los patrones específicos. Los más exitosos utilizan una combinación de varios clasificadores diferentes.

Elegir una técnica de indexación por separado por lo general no es suficiente; una estrategia de recuperación también se define usualmente de acuerdo a la aplicación de los requerimientos, tales como la exactitud y eficiencia deseada o el involucramiento de una persona humana en el proceso de revisión, entre otros.

En general, pueden definirse estrategias diferentes para el mismo mecanismo. Por ejemplo, la búsqueda puede detenerse cuando una porción fija de la base de datos ha sido explorada o en la medida que se encuentre una huella dactilar coincidente.

Los diseñadores de algoritmos usualmente adquieren o recolectan su propia base de datos de huellas dactilares y evalúan la exactitud de sus algoritmos de huella dactilar en esta base de datos. Al evaluar nuevos algoritmos,

o cambios en alguno ya probado, los expertos tratan de entender si un cambio mejora los falsos positivos, falsos no concordantes, ambos o ninguno y por qué. Los diseñadores de algoritmos pueden desarrollar técnicas algorítmicas para abordar los errores restantes y mejorar la exactitud de los algoritmos. Las organizaciones públicas (por ejemplo, el NIST) llevan a cabo pruebas periódicas de algoritmos de huella dactilar por parte de diferentes proveedores en una base de datos común para juzgar su exactitud relativa.

Existe una compensación entre las relaciones de errores de tipo falso positivo y falso no concordante dentro del emparejamiento de huella dactilar. Las diferentes aplicaciones tienen diferentes requerimientos para estos dos tipos de errores. Curiosamente, los algoritmos de huella dactilar diferentes pueden trabajar de manera distinta, dependiendo de las relaciones de errores. Por ejemplo, el algoritmo A puede ser mejor que el algoritmo B en una relación falsa positiva baja, pero el algoritmo B puede ser mejor que el algoritmo A en una relación falsa no concordante. En tales casos, los diseñadores de algoritmos pueden elegir cierto algoritmo o parámetros específicos para utilizarse, dependiendo de la aplicación.

4.3. Tecnología MEGAMATCHER

4.3.1. Introducción y antecedentes

La tecnología de MegaMatcher [11] está diseñada para AFIS de gran escala y para desarrolladores de sistemas biométricos que manejan diferentes tipos de datos, tales como las huellas dactilares, el reconocimiento facial, la lectura de iris, el registro de voz o las impresiones palmares, entre otros. En general, esta tecnología garantiza un nivel de confiabilidad relativamente alto en relación con los estándares del mercado actual, así como una velocidad más que aceptable para la identificación biométrica, incluso cuando se utilizan grandes bases de datos.

Se trata de una tecnología propiedad de Neurotechnology, compañía fundada en Vilnius, Lituania, en 1990, con la idea principal de utilizar redes neuronales para aplicaciones orientadas a la identificación biométrica de

[11] Ref. Bibliográfica [11] https://www.neurotechnology.com/about.html y su brochure institucional en https://download.neurotechnology.com/Neurotechnology_Brochure_2019-09-13.pdf

personas, robótica e inteligencia artificial. En 1991, un año después de la fundación, la compañía lanzó el primer sistema de identificación de huellas digitales para investigaciones criminales, posteriormente, en 1997, ya había logrado extenderse al uso civil para sus aplicaciones biométricas.

Una vez que la empresa comprendió los beneficios de fusionar varias modalidades biométricas, dirigió sus esfuerzos hacia la construcción de un producto multibiométrico, el cual fue lanzado en 2005 bajo el nombre de MegaMatcher Software Development Kit, circunscripto al reconocimiento de huellas digitales y rostros en esa primera versión.

En la actualidad, la empresa acumula más de 200 productos y clientes entre los que se encuentran más de 3000 integradores de sistemas, empresas de seguridad y proveedores de hardware en más de 140 países.

De acuerdo a lo informado por ANSES, es la tecnología MegaMatcher la que está siendo utilizada en la base de datos con las plantillas de minucias de huellas dactilares de Mi Huella. Por ello, se estudiarán las características generales de esta tecnología tratando de contextualizarlas, en la medida de lo posible, al caso de ANSES.

4.3.2. Principales componentes y arquitecturas de MegaMatcher

La tecnología está disponible para el desarrollo sobre plataformas Microsoft Windows, Linux, Mac OS X y Android, entre otras. El siguiente esquema muestra los componentes más importantes que la integran. A continuación, se describirán sus principales características. [12]

[12] Referencia Bibliográfica [12] http://neurotechnology.com.ar/megamatcher-references.html y Brochure de MegaMatcher SDK en https://download.neurotechnology.com/MegaMatcher_SDK_Brochure_2019-10-03.pdf

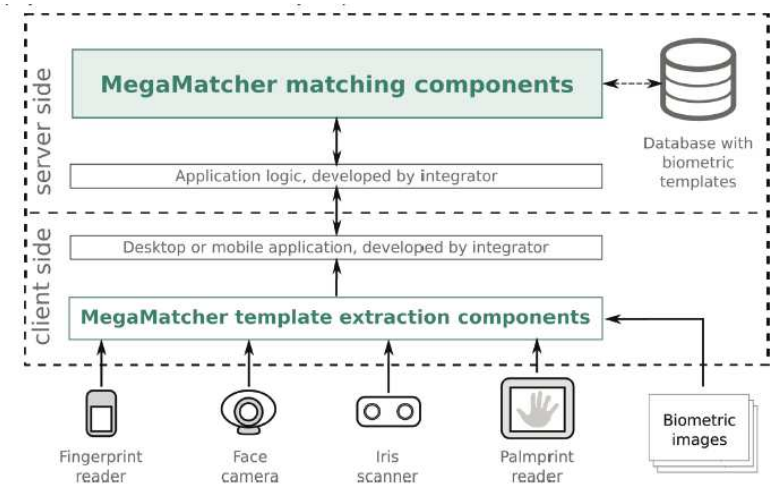


Figura 16 - Arquitectura de componentes FINGERPRINT MegaMatcher - Fuente: Ref. Bibliográfica [12]

El componente orientado a huellas dactilares (fingerprint matcher) realiza comparaciones de plantillas en los modos uno a uno o de verificación, tal como sucede con la fe de vida del sistema Mi Huella de ANSES o uno a varios, modo identificación, lo cual es lo pretendido por los programas que hacen investigación forense, por ejemplo.

En los productos promedio de mercado actuales, esta tecnología ofrece comparaciones de 40.000 huellas dactilares por segundo. Además, tales productos están diseñados para ser empleados en sistemas biométricos de escritorio o móviles tipo PC o laptops. A su vez, puede emplearse en dispositivos embebidos móviles que corren sobre Android o IOS, en cuyo caso se habla de comparaciones de hasta 3000 huellas dactilares por segundo.

Algunos productos ofrecen componentes de alta velocidad en los que la comparación crece a 200.000 huellas dactilares por segundo y están diseñados para AFIS de gran escala, que corren sobre PCs o servidores de hardware de alta gama.

Dentro de la tecnología, el componente extractor (fingerprint extractor) crea plantillas directamente desde las imágenes de las huellas dactilares. Los templates (o plantillas) de huellas dactilares pueden ser guardados con una cierta diversidad de formatos, siendo los más usuales:

- Algún formato propietario del dueño del producto ofrecido en el mercado.
- ISO/IEC 19794-2:2005 con Cor. 1:2009 Formato de datos de minucia de huellas dactilares general y en tarjeta (On Card).

- ISO/IEC 19794-2:2011 con Cor. 1:2012 Formato de datos de minucia de huellas dactilares general y en tarjeta (On Card).
- ANSI / INCITS 378-2004 Formato de datos de minucia de huella para Intercambio de Datos.

Los controles de calidad de imagen suelen aplicarse en esta tecnología para aceptar sólo imágenes de huellas dactilares de buena calidad. Por ejemplo, el extractor puede generalizar una plantilla de huellas dactilares desde varias imágenes que contienen la misma huella dactilar, con el objetivo de incrementar la calidad de la plantilla.

En su presentación de mercado más elemental, el componente extrae una plantilla de huella dactilar en algo más de un segundo. Habitualmente para lograr este desempeño, se requiere un equipo dedicado con un procesador de velocidad 2.67 GHz o superior. Sin embargo, existen componentes de alta fidelidad que realizan extracciones de plantillas a razón de 3000 huellas dactilares por minuto.

Por fin existe en esta tecnología un componente de captura (fingerprint capturer), el cual permite que las imágenes de huellas se adquieran desde lectores de huellas digitales en alguna instancia terminal del proceso o, genéricamente, del lado del cliente y luego sean enviadas para su procesamiento a un servidor que ejecuta el componente de extracción del template de minucias.

Aparentemente ésta es la opción elegida por el sistema Mi Huella de ANSES, donde las imágenes de las huellas dactilares capturadas y enviadas por las entidades bancarias residen en una base de datos en su formato de imagen y las minucias en otra, bajo tecnología MegaMatcher. Seguidamente, se muestra el esquema de componentes que corresponde a ese diseño.

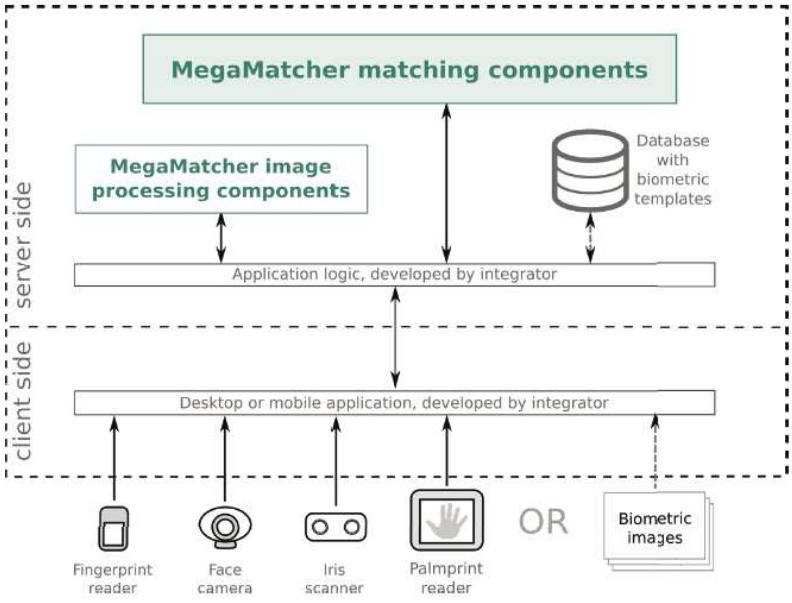


Figura 17. Arquitectura con FINGERPRINT EXTRACTOR en el servidor. Fuente: Ref. Bibliográfica [12]

Esta arquitectura está diseñada para ser utilizada en sistemas biométricos, que necesitan procesar solicitudes de un gran número de clientes en escenarios tales como banca digital, servicios electrónicos de la administración pública u otros sistemas de escala masiva. Además, en el supuesto de este tipo de arquitectura, el módulo de soporte de imágenes es compatible con diferentes formatos. En el caso de imágenes WSQ, permite la compresión de las imágenes hasta 10 o 15 veces.

El componente Fingerprint WSQ permite integrar soporte para el formato de imagen WSQ (Wavelet Scalar Quantization). El formato WSQ permite comprimir la imagen de una huella dactilar de 10 a 15 veces. El proceso de compresión WSQ acarrea pérdidas, lo que significa que la imagen reconstruida no es igual a la original. De todos modos, el algoritmo WSQ está especialmente diseñado para minimizar esas pérdidas.

Los integradores también pueden implementar la captura de imágenes por sí mismos y enviar imágenes a la parte del sistema del lado del servidor. En este caso, la implementación de aplicaciones del lado del cliente no necesita ninguna licencia para los componentes de MegaMatcher. A su vez, los componentes de extracción de plantillas de MegaMatcher se implementan en el lado del servidor del sistema biométrico.

El componente segmentador (Fingerprint Segmenter) separa las huellas dactilares de una imagen que contenga más de una, a la vez que permite extraer huellas desde registros de varios dedos escaneados o desde imágenes capturadas con escáneres que permiten procesar dos o más dedos al mismo tiempo. Con este componente viene incluido un módulo de clasificación de huellas dactilares que permite armar patrones.

Ya se señaló en el apartado correspondiente a los AFIS en general, la clasificación normalmente es usada en técnica forense, pero también puede ser empleada para incrementar la velocidad de coincidencia. Las clases definidas son:

- Curva inclinada hacia la izquierda;
- curva inclinada hacia la derecha;
- arco extendido;
- espiral;
- cicatriz;
- "desconocido" (para las clases no determinadas).

El componente de soporte biométrico estándar (Fingerprint BSS) permite integrar plantillas de huella dactilar, imágenes en formato estándar e imágenes en otros formatos con sistemas biométricos nuevos o preexistentes basados tecnologías anteriores. También permite la conversión de las plantillas patentadas por Neurotechnology con las plantillas ISO/IEC 19794-2:2005, ISO/IEC 19794-2:2011, ANSI/INCITS 378-2004, ANSI/INCITS 378-2009 y ANSI/NIST-ITL.

Además, el componente Fingerprint BSS incluye:

- Módulo de soporte de imágenes JPEG 2000 con perfiles de huellas dactilares de 1000 ppi;
- Módulo de soporte de imágenes en formato NIST.
- Módulo con el algoritmo de calidad de Imagen NIST NFIQ, el cual, ya se señaló, es el método estándar para determinar la calidad de la imagen de las huellas dactilares.

El editor de huellas dactilares latentes (Latent Fingerprint Editor) está disponible junto con el componente Fingerprint. En la mayoría de las circunstancias, el procesamiento automático de imágenes no es capaz de extraer la totalidad de la minucia o de extraer una gran cantidad de minucias falsas de una imagen de huella dactilar latente (por ejemplo, tomada de una escena de crimen). Sin embargo, un experto puede editar manualmente la plantilla de huella dactilar con el objetivo de convertirla en un AFIS para la identificación.

Dada la especificidad del anterior, es muy probable que no se encuentre integrado a la solución MegaMatcher de ANSES.

4.3.3. Medidas de recuperación de incidencias o desastres proporcionadas por MegaMatcher

Las licencias de recuperación ante desastres para los componentes del lado del servidor MegaMatcher están destinadas a usarse en el contexto de una incidencia de alcance masivo y graves consecuencias, por medio de centros ad hoc (CDR), es decir centros de recuperación de desastres.

Un CDR es un sitio contingente o alternativo que tiene el mismo equipamiento informático que el sitio principal, que refleja los datos del entorno del sitio primario en forma completa como en un espejo y está en espera mientras el sitio primario está funcionando. Si el sitio primario falla, el CDR se hace cargo de las operaciones.

La empresa propietaria de MegaMatcher proporciona o pone a disposición licencias para recuperación de desastres del tipo descripto. Inclusive se promocionan a través de diferentes presentaciones comerciales.

En el caso del sistema Mi Huella, que utiliza esta tecnología, no se ha informado la suscripción de este tipo de licencias y la contingencia pareciera estar atendida por medio de la distribución de la base biométrica en cada entidad del sistema de pagos de beneficios previsionales, en la medida de la cápita de beneficiarios de cada entidad.

4.4. Tecnologías de almacenamiento de datos biométricos en la Unión Europea (UE)

4.4.1. Premisas y fundamentos para la protección de datos personales en general

La conservación o permanencia en algún lugar de almacenamiento de los datos personales están sujetas según el Reglamento General para la Protección de Datos de la UE (RGPD) a las siguientes premisas y fundamentos [13]

- Los datos personales son cualquier información relativa a una persona física viva identificada o identificable.
- Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.
- Los datos personales que hayan sido anonimizados, cifrados o presentados con un seudónimo, pero que puedan utilizarse para volver a identificar a una persona, siguen siendo datos personales.
- Los datos personales que hayan sido anonimizados**,** de forma que la persona no sea identificable o deje de serlo, dejarán de considerarse datos personales. Para que los datos se consideren verdaderamente anónimos, la anonimización debe ser irreversible.

A la vez, el RGPD protege los datos personales independientemente de la tecnología utilizada para su tratamiento. En ese sentido, podría decirse que se pretende tecnológicamente neutro y se aplica tanto al tratamiento automatizado como manual, siempre que los datos se organicen con arreglo a criterios predeterminados (como el orden alfabético).

A partir de lo anterior, podemos ver cómo la anonimización de los datos personales es una de las medidas de protección que la Unión Europea ha impulsado con mayor vehemencia.

4.4.2. El modelo recientemente propuesto para datos biométricos

Se presenta a continuación un documento desarrollado por la Comisión Europea que trata de una propuesta de reglamento de interoperabilidad de sistemas orientados a la gestión de migraciones, control de fronteras y seguridad, el cual adquiere relevancia por la circunstancia de que su núcleo es un sistema de

[13] Ref. Bibliográfica [13] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es Sitio oficial de la Unión Europea, acerca de Protección de Datos.

identificación biométrica y por ello permite apreciar cuáles son las premisas fundamentales a tener en cuenta sobre el tratamiento y almacenamiento de los datos biométricos [14]

El contexto de la propuesta del nuevo reglamento atiende a los recientes y graves retos que han llevado a la UE a unificar y reforzar sus herramientas de información para la gestión de las fronteras, la migración y la seguridad. Sin embargo, pese a la gravedad de los hechos que dan origen a estas acciones, la reforma se da en el marco del pleno respeto de los derechos consagrados en la Carta de los Derechos Fundamentales de la UE, en particular el derecho a la protección de los datos personales.

Los objetivos específicos del reglamento son:

- Asegurarse de que los usuarios finales, en particular la guardia de fronteras, la policía, los funcionarios de inmigración y las autoridades judiciales, dispongan de un acceso rápido, ininterrumpido, sistemático y controlado a la información que necesitan para desempeñar sus tareas.
- Ofrecer una solución para detectar identidades múltiples relacionadas con el mismo conjunto de datos biométricos, tanto para garantizar la correcta identificación de las personas de buena fe, como combatir la usurpación de identidad.
- Facilitar los controles de identidad de los personas provenientes de países externos a la UE
- Racionalizar el acceso de los cuerpos policiales a los sistemas de información no policiales a escala de la UE.

Además de estos objetivos operativos principales, la propuesta debe contribuir a reforzar y racionalizar las condiciones de seguridad y protección de datos que rigen los sistemas respectivos, así como a mejorar y armonizar los requisitos de calidad de sus datos.

Los tres sistemas de información centralizados existentes al momento de la propuesta son:

- Sistema de Información de Schengen (SIS), con un amplio espectro de descripciones de personas (denegaciones de entrada o de estancia en la UE, órdenes de detención europeas, personas desaparecidas, procedimientos de asistencia judicial, controles discretos y específicos) y objetos (documentos de identidad, de viaje, perdidos, etc.)

[14] Ref. Bibliográfica [14] Comisión Europea: Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE de cooperación policial y judicial, asilo y migración - Bruselas, 13.6.2018.

- Sistema Eurodac, con los datos dactiloscópicos de los solicitantes de asilo y nacionales de terceros países que han cruzado las fronteras irregularmente.
- Sistema de Información de Visados (VIS), con datos sobre los visados para estancias de corta duración.

Además de estos sistemas existentes, se proponen en el marco del nuevo reglamento, tres nuevos sistemas centralizados de información:

- Sistema de Entradas y Salidas (SES), sustituto del actual sistema de sellado manual de los pasaportes, registrará electrónicamente el nombre, el tipo de documento de viaje, los datos biométricos y la fecha y el lugar de entrada y salida de los nacionales de terceros países que visiten el espacio Schengen para estancias de corta duración.
- Sistema Europeo de Información y Autorización de Viajes (SEIAV), complementario del anterior para los viajeros exentos de sellado.
- Sistema Europeo de Información de Antecedentes Penales de nacionales de terceros países (sistema ECRIS-TCN).

Para lograr la interoperabilidad que es el corazón de la propuesta, se propicia integrar los siguientes componentes:

- un portal europeo de búsqueda (PEB);
- **un servicio de correspondencia biométrica compartido (SCB compartido);**
- un registro común de datos de identidad (RCDI) y
- un detector de identidades múltiples (DIM).

El servicio de correspondencia biométrica compartido (SCB compartido) permitiría la consulta y la comparación de datos biométricos (impresiones dactilares e imágenes faciales) de varios sistemas centrales (en particular, el SIS, el VIS, Eurodac, el SES y el propuesto ECRIS-TCN). Como cada uno de los sistemas centrales (SIS, Eurodac, VIS) dispone actualmente de un motor de búsqueda de datos biométricos específico propio y el SCB compartido proporcionaría una plataforma común en la que los datos se consultarían y compararían simultáneamente.

4.4.3. Medidas y prácticas de seguridad insertas en el reglamento y sobre el SCB compartido en particular

Resulta muy interesante la controversia planteada en las discusiones preliminares de la propuesta, respecto de la necesidad de reforzar el sistema Eurodac, cuya arquitectura es técnicamente inadecuada para convertirse en parte

de la interoperabilidad de los sistemas de información, dado que únicamente almacena los datos biométricos y un número de referencia, pero no otros datos personales (por ejemplo, nombre y apellido(s), edad o fecha de nacimiento). Este planteo denota el privilegio dado hasta el momento a técnicas de anonimización de datos en el almacenamiento.

También se advierte que la utilización de datos personales que conlleva la interoperabilidad tendrá un impacto concreto en el derecho a la protección de los datos personales, ampliamente reconocido en diversos y fundamentales documentos y tratados de la Unión Europea. Sin embargo, tal como subraya el Tribunal de Justicia de la Unión Europea este derecho no es absoluto sino que considerarse en relación con su función en la sociedad, ligado al respeto de la vida privada y familiar.

Así, de conformidad con el RGPD, la libre circulación de datos dentro de la UE no se restringirá por causa de la protección de datos. Sin embargo, deberán observarse una serie de principios, basados en que cualquier limitación del ejercicio de derechos fundamentales para ser legal, debe cumplir con lo estipulado por la Carta de los Derechos Fundamentales de la UE, a saber:

- Ser establecida por la ley.
- Respetar el contenido esencial de los derechos.
- Responder efectivamente a objetivos de interés general reconocidos por la Unión.
- Ser necesaria y ser proporcional.

Seguidamente se describen los principales controles incorporados al reglamento de interoperabilidad en su conjunto y en particular respecto del SCB compartido.

4.4.3.1. Controles respecto del almacenamiento de datos biométricos

El SCB compartido generaría importantes beneficios al basarse en un único componente tecnológico en lugar de cinco diferentes. No obstante, los datos biométricos, es decir, las impresiones dactilares e imágenes faciales, se conservarían exclusivamente en los sistemas subyacentes. Para ello, el SCB compartido crearía y conservaría una representación matemática de las muestras biométricas (una plantilla), pero se desprendería de los datos reales, que seguirían, por lo tanto, almacenándose en un lugar, una sola vez.

El SCB compartido sería una ayuda fundamental para detectar conexiones entre conjuntos de datos y las diferentes identidades asumidas por una misma persona en distintos sistemas centrales.

A su vez, mediante la creación de un registro común de datos de identidad (RCDI) se tendría el componente compartido para almacenar los datos de identidad biográficos y biométricos de los nacionales de terceros países registrados en Eurodac, el VIS, el futuro SES y los propuestos SEIAV y ECRIS-TCN. Cada uno de estos cinco sistemas centrales registra o registrará los datos biográficos de personas concretas por motivos específicos. Los datos de identidad pertinentes se almacenarían en el RCDI, pero seguirían perteneciendo de manera principal a los respectivos sistemas subyacentes que hubieran registrado estos datos.

También se señala en el reglamento que las plantillas biométricas quedarán almacenadas en el SCB compartido tanto tiempo como los datos biométricos correspondientes estén almacenados en los sistemas subyacentes. Esto implica un pronunciamiento claro y restrictivo respecto de los tiempos de guarda.

4.4.3.2. Controles en relación con el acceso a los datos

A los efectos de extremar los cuidados en el acceso a los datos personales, se prevé implementar una funcionalidad, denominada aviso de respuesta positiva, utilizando una consulta de datos en dos fases.

En una primera fase, un agente de policía iniciaría una consulta sobre una persona concreta, utilizando los datos de identidad, el documento de viaje o los datos biométricos de esa persona, para comprobar si el RCDI almacena información sobre la persona buscada. Cuando haya información, el funcionario recibirá una respuesta que indique cuáles contienen datos sobre esa persona (el aviso de respuesta positiva).

De esta manera, a priori, el funcionario no tendría acceso a los datos contenidos en ninguno de los sistemas subyacentes, pero en una segunda fase, podría solicitar dicho acceso, de conformidad a la normativa vigente y los procedimientos establecidos por cada sistema y por su respectiva instrumentación en cada Estado miembro.

De esta manera, la propuesta limita el tratamiento de datos a lo necesario para el propósito específico, concede acceso únicamente a aquellas entidades que “necesitan saber”, con la debida autorización competente y los plazos de conservación de datos (en su caso) son adecuados y limitados.

4.4.3.3. Controles en relación con la conservación de los registros de acceso y operación

La conservación de los registros de todas las operaciones de tratamiento de datos dentro de los diferentes componentes, es una de las medidas de seguridad que la propuesta de reglamento de interoperabilidad implementa con meticulosidad. En virtud de ello, se reitera ante cada componente cuál es la información de seguimiento o control de las operaciones que deberá registrarse. En términos generales, se proponen los siguientes datos para todos y cada uno de los componentes del reglamento:

- la autoridad del Estado miembro y el usuario individual del componente, incluido el perfil utilizado, que accede a la consulta u operación,
- la fecha y hora de la consulta,
- la finalidad o el motivo del acceso del usuario,
- el tipo de datos utilizados para iniciar la consulta,
- los resultados de la consulta,
- la marca identificadora de la persona que haya realizado la consulta, de conformidad con las normas de la UE.

En el caso del componente SBC compartido, se agregan los siguientes:

- el historial de la creación y el almacenamiento de las plantillas biométricas;
- una referencia a los sistemas de información de la UE consultados con las plantillas biométricas almacenadas en el SCB compartido;
- el tipo de datos biométricos utilizados para iniciar la consulta;
- la duración de la consulta y la fecha y hora de los resultados.

Los registros únicamente podrán utilizarse para la supervisión de la protección de datos. Dichos registros estarán protegidos por medidas adecuadas contra acceso no autorizado y serán suprimidos un año después de su creación, salvo que sean necesarios para procedimientos de supervisión que ya hayan dado comienzo.

4.4.3.4. Controles relacionados con la calidad de los datos biométricos

Señala la propuesta de reglamento que las plantillas biométricas solo podrán introducirse en el SCB compartido tras un control de calidad automatizado de los datos biométricos añadidos a alguno de los sistemas de información con que cuenta el SCB compartido, a los efectos de cerciorar que se alcanza un estándar mínimo de calidad de los datos.

De esta manera se determina que el almacenamiento de los datos cumplirá determinados estándares que están establecidos en el propio reglamento.

4.4.3.5. Imperativos en el diseño de los planes de seguridad

El responsable del desarrollo del sistema de interoperabilidad, así como los Estados miembros adoptarán las medidas necesarias, incluidos un plan de seguridad, un plan de continuidad de las actividades y un plan de recuperación en caso de catástrofe, a fin de:

- proteger los datos físicamente, entre otras cosas mediante la elaboración de planes de emergencia para la protección de las infraestructuras críticas;
- impedir la lectura, copia, modificación o retirada no autorizadas de los soportes de datos;
- impedir la introducción no autorizada de datos y la inspección, modificación o eliminación no autorizadas de datos personales registrados;
- impedir el tratamiento no autorizado de datos y la copia, modificación o eliminación no autorizadas de datos;
- garantizar que las personas autorizadas para acceder a los componentes de interoperabilidad tengan únicamente acceso a los datos cubiertos por su autorización de acceso, exclusivamente mediante identidades de usuario individuales y modos de acceso confidenciales;
- garantizar la posibilidad de verificar y determinar a qué organismos pueden transmitirse datos personales mediante equipos de transmisión de datos;
- garantizar la posibilidad de verificar y determinar qué datos han sido tratados en los componentes de interoperabilidad, en qué momento, por quién y con qué fin;
- impedir la lectura, copia, modificación o eliminación no autorizadas de datos personales durante su transmisión hacia o desde los componentes de interoperabilidad o durante el transporte de soportes de datos, en particular mediante técnicas adecuadas de cifrado;

Además de todas las anteriores, el reglamento propone otras medidas de seguridad al retomar desde su articulado, cuestiones relativas al ejercicio del

derecho de acceso a la información y rectificación de datos personales, así como a los recaudos para la preservación de la confidencialidad sobre los datos accedidos en el ejercicio de la función respectiva.

4.5. Conclusiones preliminares sobre tecnologías de biometría

En primer término, es necesario reflexionar acerca del papel de la calidad en los sistemas de huellas dactilares, en particular en relación con la exactitud de los algoritmos que conllevan los procesos de extracción de plantillas de minucias y luego de emparejamiento o comparación entre las mismas. Esta calidad es crucial en el diseño de sistemas de huella dactilar para el uso en la vida real. El resultado del emparejamiento debe ser confiable porque muchas decisiones de la vida real se basarán en él.

Otra distinción que debe realizarse cuanto antes es la relativa a la finalidad que persiguen los sistemas de huellas dactilares como una de las expresiones más representativas y usuales de los datos biométricos. No da lo mismo un sistema orientado a cuestiones forenses o de control migratorio, que un sistema donde la huella dactilar es el mecanismo elegido para corroborar una identidad. En el primer caso, la búsqueda es uno a varios (cientos de miles, quizás) mientras que en el otro, es uno a uno (se tiene una huella fresca correspondiente a una persona y se corrobora que corresponda con la existente en la base de datos para la misma persona).

El diseño y por ende la calidad de los algoritmos de obtención de la imagen, de extracción de características y de comparación (o emparejamiento) dependen sobremanera de cuál sea el propósito del sistema. En algunos casos se privilegiarán la celeridad y la flexibilidad de los procedimientos de búsqueda y comparación, mientras que en otros, el énfasis estará en la precisión de la coincidencia y la baja tasa en los errores tipificados como falsos positivos y falsos negativos, simultáneamente.

Claramente, el sistema Mi Huella corresponde a un AFIS orientado a la verificación de identidades, de eso se trata la fe de vida que se tramita por medio de él.

La tecnología propietaria MegaMatcher, una de las más relevantes en todo el mundo, es adecuada para cualquiera de las dos vertientes (modo búsqueda de identidad o modo verificación) y por lo que puede apreciarse a través del modelo de datos informado, la implementación realizada en ANSES se adapta a lo que el sistema MiHuella requiere. En ese sentido, el componente fingerprint matcher realiza comparaciones de plantillas en el modo verificación. Bajo esta modalidad, la tecnología ofrece tasas de rendimiento muy altas, por un lado en cuanto a capacidad de procesamiento (comparaciones de 40.000 huellas dactilares por segundo) y por el otro, en relación con el tiempo requerido en el dispositivo de lectura para obtener la imagen. Sin embargo, la arquitectura implementada en Mi Huella vuelve irrelevante esta velocidad dado que independiza los procesos y permite que las imágenes de huellas se adquieran desde lectores de huellas digitales en alguna instancia terminal del proceso (genéricamente, del lado del cliente que en este caso son las entidades bancarias de pago) y luego sean enviadas para su procesamiento a un servidor que ejecuta el componente de extracción del template de minucias.

Aparentemente ésta es la opción elegida por el sistema Mi Huella de ANSES, donde las imágenes de las huellas dactilares capturadas y enviadas por las entidades bancarias residen en una base de datos en su formato de imagen y las minucias en otra, bajo tecnología MegaMatcher.

Además, en el supuesto de este tipo de arquitectura, el módulo de soporte de imágenes es compatible con diferentes formatos. En el caso de imágenes WSQ, que son las utilizadas por Mi Huella, permite la compresión de las imágenes hasta 10 o 15 veces, con una pérdida de precisión mínima.

Cabe destacar que la implementación de aplicaciones para la captura de imágenes del lado del cliente no necesita ninguna licencia para los componentes de MegaMatcher.

Por fin, la propuesta de reglamento de la UE para la interoperabilidad de sistemas basados en datos personales y biométricos ilustra ampliamente acerca de las tecnologías a emplear y las medidas de seguridad que las mismas requieren, facilitan o promueven. A partir de esta información es posible reflexionar sobre estas cuestiones en forma comparativa respecto del sistema Mi Huella.

Sobre la anonimización, aspecto clave para la protección de los datos personales, por lo visto en el caso del RGPD y también respecto de la propuesta de reglamento para la interoperabilidad de sistemas biométricos, es posible señalar que las bases de datos de Mi Huella están bastante alejadas de ese concepto. La base SBS contiene en el mismo modelo de datos, las imágenes de las huellas dactilares y los datos de identificación de las personas titulares de esas huellas. En otra base, están las plantillas de las huellas y nuevamente datos de identidad de los titulares.

Por fin, también deberíamos preguntarnos si es correcto y apegado al espíritu de la ley PDP de Argentina la proliferación de bases de datos en las entidades bancarias, ya sea como resguardo para una eventual contingencia o simplemente como stock formado durante la transmisión de las imágenes de las huellas en el proceso de enrolamiento.

También, analizando las dos bases de datos SIA y SBS, una con las huellas en imágenes y otra con las plantillas y la marca MegaMatcher, es posible inferir que la incorporación de esta última es más o menos reciente y que los datos biométricos localizados en las entidades bancarias son residuales del proceso de enrolamiento en el marco de la base SBS.

Otra cuestión a reflexionar es la relativa a los tiempos de guarda de los datos biométricos. Deberíamos preguntarnos si en Mi Huella existe algún protocolo al respecto. En apariencia, no es el caso.

Como última reflexión vale la mención de la importancia que adquiere para la UE la conservación de la bitácora de los accesos a la base de datos y a los diferentes sistemas de datos biométricos. Ello a los efectos de realizar un seguimiento estrecho de la operatoria, como aspecto disuasivo de eventuales accesos indebidos y como pista de auditoría en el caso de que efectivamente se produzcan.

Capítulo IV – CONCLUSIONES, RECOMENDACIONES Y PRÓXIMOS PASOS

5.1. Hipótesis verificadas, hallazgos y conclusiones

De acuerdo a lo que se expuso en apartados precedentes, el desarrollo del presente trabajo se ha basado en las siguientes hipótesis:

- El marco normativo existente es insuficiente en cuanto a la cobertura y orientación sobre la protección que ofrece para datos personales en general y biométricos en particular.
- En virtud de esa insuficiencia y de cierto retraso respecto de la evolución de determinadas tecnologías, además del uso creciente alcanzado por las mismas, podría tipificarse ese marco como poco robusto o directamente inmaduro.
- Existen oportunidades de mejora en relación con las tecnologías en uso para el almacenamiento de datos biométricos y el grado de protección que estas ofrecen para esos datos, tomando en cuenta los principales riesgos a los que están expuestos.
- A su vez, la comprensión de tales mejoras tecnológicas podrían impactar en el marco normativo que se supone débil y contribuir a su fortalecimiento.

5.1.1. En relación con el marco normativo argentino actual

En relación con el marco normativo, a lo largo de la realización de los respectivos estudios que se fueron presentando en los apartados anteriores, es posible identificar los siguientes hallazgos que refuerzan la primera de las hipótesis planteadas:

1. El instituto relativo a la protección de los datos biométricos en tanto datos personales existente en Argentina, recoge un mandato expreso de la Constitución Nacional, no obstante lo cual, está orientado principalmente a las bases de datos públicos y del sector financiero, bancario, de la previsión social y de la salud, tanto públicos como privados.

2. Asimismo, la extensión o la amplitud que aparentemente incorpora la reglamentación en relación con el concepto de archivos, registros o bancos de datos afectados no incide ni causa efectos prácticos en las bases de datos personales de origen o de finalidad privadas, por fuera de los sectores enunciados en el párrafo anterior.
3. De esta manera, la legislación argentina actual no se expresa sobre aspectos vinculados al almacenamiento de datos personales, tales como medios, métodos o formas. Esta omisión puede hacerse extensiva a las medidas de protección, dado que sólo existe una mención muy general en relación con la seguridad o la preservación de la integridad y la confidencialidad de los bancos de datos y sobre a quién corresponde esa responsabilidad.
4. Este déficit normativo no alcanza a cubrirse con las resoluciones de la AAIP, que solo enfocan el tema desde la perspectiva de una consideración superficial respecto de la evolución y la diversidad tecnológicas, a las que señalan como vertiginosas. Por ello, resultan insuficientes en los hechos, sobre todo en relación con la diversidad tecnológica que pretenden abarcar.
5. La ley no distingue a los datos biométricos dentro de los datos personales y si bien este concepto aparece recientemente tratado en una de las guías de criterios orientadores de la AAIP, en un esfuerzo claramente orientado a la modernización de la normativa, todavía no se pronuncia sobre ninguna cuestión relacionada con su tratamiento, registro, almacenamiento o conservación de los datos.

Por otra parte, se evaluó la efectividad del marco normativo para la protección de los datos biométricos, entendida como una medida de qué tan obligada al cumplimiento de la ley está la sociedad en su conjunto y en particular los responsables de bases o bancos de datos personales y biométricos. De dicha valoración surgen las siguientes conclusiones:

1. Una primera constatación verifica que la ley de AIP que sucede a la de PDP y de alguna manera es instrumentadora de ésta, aporta mayor efectividad a los procedimientos que ponen en ejecución los derechos de los titulares sobre sus datos personales, debido a la

elevación del rango institucional del organismo que tutela ambas legislaciones, ascendido desde el nivel de una dirección nacional en un ministerio al de agencia estatal en la órbita de la Jefatura de Gabinete de Ministros.

2. Refuerza lo anterior el conjunto de criterios y guías de procedimientos que despliega la Agencia, instrumentando y facilitando el ejercicio del derecho de acceso a los datos personales (el recurso de hábeas data) como si fuera un caso especial de las solicitudes de acceso a la información pública. De esta manera se aprovecha para el caso de la PDP a todo el conjunto de recursos dispuestos en torno de la tutela del acceso a la información pública, tales como agentes coordinadores del trámite en cada jurisdicción, mecanismos de tramitación a distancia y manuales de procedimientos que establecen pasos, responsables, tareas y plazos.
3. Asimismo, el régimen de control de cumplimiento y eventual aplicación de sanciones previsto en el origen de la legislación de PDP y actualizado en el año 2010, alcanza plena vigencia a partir del accionar sistemático de la AAIP como órgano de control y resolución de recursos y descargos. No obstante, la percepción pecuniaria de las sanciones y multas impuestas no sucede con la frecuencia o en los tiempos que cabría esperar, relativizando así la efectividad del régimen de control en su conjunto.
4. En el año 2019, la AAIP avanza en la actualización del régimen de protección de datos personales, al publicar criterios orientadores e indicadores de mejores prácticas en consonancia con algunos de los promocionados por el Reglamento General de Protección de Datos de la Unión Europea (GDPR).
5. Asimismo, como siguiente etapa del proceso de actualización aludido, debe mencionarse el impulso del proyecto de modificación de la Ley N° 25.326 inspirado en el GDRP (el cual estaba en tratamiento parlamentario hasta el 1 de marzo de 2020) y la emisión de nuevas reglamentaciones alineadas con éste por parte de la AAIP.

5.1.2. En relación con el marco normativo argentino proyectado

Es de gran interés apreciar cuáles son los aspectos proyectados por la nueva legislación y los introducidos por la vía reglamentaria, a la espera de su consolidación en la futura modificación. Esta perspectiva también brinda una valoración acerca de cuan efectivo y adecuado respecto de las tecnologías resulta el cuerpo legal actual.

1. En líneas generales, el proyecto de ley garantiza los derechos de los titulares de los datos, aclara cuáles son las bases legales para el tratamiento de datos, añade el interés legítimo del responsable del tratamiento, entre otras bases legales, al consentimiento del titular de los datos ya legislado y genera obligaciones a los responsables del tratamiento de datos que son consistentes con el objeto de la norma proyectada: la protección integral de los datos personales a fin de garantizar el ejercicio pleno de los derechos de sus titulares.
2. En la elaboración de la norma proyectada se ha seguido la tendencia internacional en la materia, estableciendo que la normativa se aplicará en distintos supuestos, aun cuando, bajo ciertas condiciones, los responsables de tratar los datos no se encuentren en territorio nacional.
3. Asimismo, el proyecto incorpora obligaciones para los responsables del tratamiento de datos tales como notificar incidentes de seguridad; realizar evaluaciones ex ante de riesgos e impactos ante proyectos o medidas de tratamiento nuevas, o adoptar medidas para el cumplimiento de la ley que sean proporcionales a las modalidades, finalidades, contexto, tipo y categoría de datos tratados o por tratar.
4. Se crea la figura del delegado de protección de datos cuya designación es obligatoria en el caso de autoridades u organismos públicos, en el de tratamiento de datos sensibles como parte de la actividad principal del responsable y en el tratamiento de datos a gran escala.
5. El proyecto de ley da cabida a derechos de los titulares de los datos que hasta ahora no habían sido reconocidos tales como el derecho a

la portabilidad de datos, a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, a solicitar la supresión de sus datos personales de las bases de datos (siempre que la supresión no se oponga al ejercicio de la libertad de expresión e información) y, en el caso de niñas, niños y adolescentes, incorpora parámetros especiales para el tratamiento de datos de acuerdo a la Convención sobre los Derechos del Niño.

Por fin, en relación con el almacenamiento, el registro o la conservación de los datos, el proyecto avanza en varias cuestiones, dejando al descubierto y de un modo elocuente los aspectos pendientes de tratamiento o deficitarios de la legislación actual.

- Impulsa un nuevo principio de seguridad, el cual señala que el responsable o el encargado del tratamiento de los datos, deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y la confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, considerando ciertos factores como el riesgo inherente por el tipo de dato personal; si los datos son sensibles, el desarrollo tecnológico; las posibles consecuencias de un incidente de seguridad y los registros de incidentes previos.
- El proyecto no menciona expresamente a la biometría ni a los datos biométricos, sin embargo, el nuevo principio de seguridad comprende algunas de sus distinciones y gran parte de su problemática, sobre todo en relación con los temas de portabilidad ante el tratamiento electrónico de datos personales, o los criterios de protección desde el diseño y por defecto, aplicados a la cantidad y calidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Medidas que deben garantizar que, por defecto, los datos personales no sean accesibles sin autorización del titular, a un número indeterminado de personas humanas.
- Otra fortaleza buscada a través del nuevo orden legal refiere a la previsión de llevar a cabo supervisiones y auditorías internas o externas que demuestren ante la autoridad de control cuáles son los mecanismos de

autorregulación y las medidas concretas tomadas para el cumplimiento de la responsabilidad de protección. Asimismo, el proyecto prevé que la evaluación de impacto será obligatoria en los casos de elaboración de perfiles, tratamiento de datos sensibles a gran escala o de datos relativos a antecedentes penales o contravencionales. Esto último comprende de manera tácita a datos de tipo biométrico, con lo cual queda en claro que están comprendidos en los alcances la normativa.

Hasta este momento hemos obtenido conclusiones respecto de cómo ha ido evolucionando el ordenamiento legal vigente y cuál es el proyectado. También es posible concluir que por el momento, la materialización del proyecto es incierta y que probablemente por eso mismo, la AAIP ha pretendido sustanciar parte de sus previsiones en reglamentaciones emitidas en el último tiempo.

5.1.3. En relación con el marco normativo argentino comparado con el de la UE

También con criterio comparativo, es posible obtener otras conclusiones en relación con las tecnologías a emplear en el tratamiento de datos biométricos y las medidas de seguridad promovidas por la UE. Seguidamente, las principales:

1. La anonimización deviene un aspecto clave para la protección de los datos personales que es fuertemente impulsado tanto por el RGPD como por los reglamentos operativos y sobre la interoperabilidad de sistemas biométricos. En la legislación local, tanto vigente como proyectada, este aspecto prácticamente no está tratado. Como ejemplo de aplicación, el caso Mi Huella, da sobradas evidencias de lo alejadas que están sus bases de datos de este concepto. Tal como se señaló en apartados anteriores, la base SBS contiene en el mismo modelo de datos, las imágenes de las huellas dactilares y los datos de identificación de las personas titulares de esas huellas. En otra base, están las plantillas de las huellas y nuevamente datos de identidad de los titulares.
2. Otro factor crítico es el relativo a la limitación de los ámbitos de almacenamiento de datos y de sus plazos de conservación. Mientras que las reglamentaciones europeas destacan el tema y son

prolíficas en reglamentaciones que lo abordan con un tratamiento riguroso, la legislación argentina prácticamente lo ignora. Como evidencia de este déficit podemos señalar lo sucedido con las bases de datos biométricos en poder de las entidades bancarias, sobre las que no está en claro si fueron originalmente previstas como el resguardo de una eventual contingencia o han quedado como un excedente natural de la transmisión de las imágenes de las huellas cuando el proceso de enrolamiento no estaba centralizado en ANSES.

3. Cualquiera sea el origen de tal acumulación, no existe por el momento ninguna previsión legal respecto de las responsabilidades por su almacenamiento o guarda y en qué condiciones de seguridad debería darse. Tampoco existe un ordenamiento que obligue a su decomiso actual, ahora que las bases de datos están aparentemente centralizadas en ANSES.
4. En cuanto a los tiempos de conservación de los datos biométricos en las bases de datos, tampoco la legislación argentina ni las reglamentaciones de la AIIP avanzan concretamente sobre este aspecto, pese a la relevancia que adquiere en la normativa europea, que advierte de los riesgos implicados en la proliferación indiscriminada de datos, facilitada esta circunstancia por la cada vez más asequible tecnología y el equipamiento cada vez más económico.
5. Como evidencia, nuevamente es posible referirnos al caso bajo estudio, donde no se ha apreciado procedimiento o protocolo alguno referido a cuánto tiempo se deben mantener los datos biométricos, por ejemplo, luego del fallecimiento de su titular. Sabemos que se inhabilita el cobro del beneficio en el caso de fallecimiento, precisamente porque el titular no puede presentar su huella dactilar ante el escáner, pero no sabemos qué se hace con los datos biométricos que han quedado guardados en las bases de datos centrales de ANSES o en las periféricas del sistema bancario. Mucho menos, en qué plazos.

6. Finalmente, como última reflexión surgida a partir de la comparación entre los cuerpos normativos europeo y argentino, es dable mencionar la importancia dada por el primero de ellos al registro de auditoría de accesos a la base de datos y a los diferentes sistemas de datos biométricos; aspecto que en la normativa argentina aparece directamente soslayado y en el mejor de los casos librado al conocimiento de buenas prácticas que puedan tener los responsables de las áreas informáticas que traten datos biométricos.

5.1.4. Hipótesis primera y segunda verificadas

Los apartados anteriores han expuesto un conjunto de aspectos del marco normativo en vigencia que no dejan dudas acerca de su insuficiencia en cuanto a la efectividad de la protección que ofrece, para datos personales en general, biométricos en particular y más en lo específico, para los aspectos relativos a su tratamiento o a su almacenamiento.

Al momento de pronunciarse sobre la segunda hipótesis es conveniente recordar que desde la sanción de la Ley N° 25.326 la tecnología ha venido evolucionado a un ritmo vertiginoso, impactando en gran medida en la protección de los datos personales y trayendo enormes desafíos en el campo del ejercicio de los derechos. Por un lado, beneficios innegables y por el otro, riesgos sobre la privacidad cada vez más acuciantes.

Todo lo dicho hasta el momento permite señalar que se está en presencia de un marco normativo todavía inmaduro, poco adecuado a los cambios de paradigma tecnológico que marcan una evolución permanente y con un ritmo cada vez más acelerado, en vías de ser actualizado y perfeccionado mediante una instancia legislativa que aún no se ha concretado.

5.2. Oportunidades de mejora y recomendaciones finales

A partir de los postulados de la tercera y cuarta hipótesis, enunciamos los conceptos finales del presente trabajo.

En primer término, es necesario reflexionar acerca del papel de la calidad en los sistemas de huellas dactilares, en particular en relación con la exactitud de los algoritmos que conllevan los procesos de extracción de plantillas de minucias

a los efectos de mejorar los procesos de comparación (emparejamiento) entre las mismas. Esta calidad es crucial en el diseño de sistemas de huella dactilar para el uso en la vida real, dado que las decisiones a tomar se basan en resultados de comparaciones que deben ser confiables.

La otra distinción de importancia es la relativa a la finalidad que persiguen los sistemas de datos biométricos. Los hay orientados a cuestiones forenses o de control migratorio, es decir, sistemas donde la huella dactilar es el mecanismo elegido para descubrir o corroborar una identidad. En estos casos, la búsqueda es uno a varios (cientos de miles, quizás). El otro gran grupo a tener en cuenta es el relativo a los sistemas de verificación de identidad, que son aquellos en los que se tiene una huella fresca correspondiente a una persona y se verifica que corresponda con la existente en la base de datos para la misma persona. Cabe destacar que la mayor parte de los sistemas biométricos son de este tipo, prácticamente todos los utilizados en ámbitos no gubernamentales y gran parte de los usados en la esfera de gobierno.

El diseño y por ende la calidad de los algoritmos de obtención de la imagen, de extracción de características y de comparación dependen sobremanera de cuál sea el propósito del sistema. En algunos casos se privilegiarán la celeridad y la flexibilidad de los procedimientos de búsqueda y comparación, mientras que en otros, el énfasis estará en la precisión de la coincidencia y la baja tasa en los errores tipificados como falsos positivos y falsos negativos, simultáneamente.

De esta manera, las principales oportunidades de mejora a través de las tecnologías sobrevienen de la mano de la calidad, enmarcada en alguno de estos dos diseños u orientaciones básicos. Asimismo, como en la mayor parte del presente trabajo, las valoraciones sobre las mejoras tecnológicas están contrastadas con el caso de estudio elegido.

Claramente, el sistema Mi Huella corresponde a un AFIS orientado a la verificación de identidades a través del trámite correspondiente a la fe de vida del derechohabiente. La tecnología que se utiliza en él, MegaMatcher (de carácter propietario), es una de las más relevantes en todo el mundo, a la vez que adecuada para cualquiera de las dos vertientes, modo búsqueda de identidad o

modo verificación, siendo la implementación realizada en ANSES de este segundo tipo, en consonancia con lo que el sistema MiHuella requiere.

En ese sentido, el componente fingerprint matcher realiza con excelente desempeño de tiempo las comparaciones de plantillas en el modo verificación. Las imágenes de huellas que se adquieran desde lectores de huellas digitales dispuestos en las entidades bancarias de pago, luego son enviadas para su procesamiento a un servidor que ejecuta el componente de extracción de la plantilla de minucias y por fin, compara con las bases de datos de imágenes reclutadas en el formato de minucias. Bajo esta modalidad, la tecnología Megamatcher ofrece tasas de rendimiento muy altas, además de los beneficios de la compresión de imágenes con mínima pérdida de precisión.

En relación con la seguridad en las comunicaciones, las aplicaciones de enrolamiento y las del tótem del Servicio del Sistema Biométrico ANSES hacen uso de la plataforma de interconexión de ANSES, la cual se encuentra conformada por un sistema de autenticación y un sistema de autorización que permiten ejecutar las acciones del servicio SBA dentro de un nivel de seguridad aceptable, alineado con el estándar actual del mercado.

También en relación con la transmisión de imágenes de huellas, no se tiene certeza de que las mismas se envíen encriptadas, como se había previsto en un comienzo, cuando el enrolamiento se hacía desde las entidades bancarias. Aparentemente tampoco alcanzaría al caso de envío de imágenes de huellas capturadas durante el proceso de verificación o fe de vida. Sin embargo, como prácticamente la totalidad de los servicios web utilizan actualmente mecanismos de encriptación, lo más probable es que los envíos de información desde y hacia la plataforma de servicios de ANSES estén convenientemente cifrados para evitar sustracciones o intrusiones indebidas.

Asimismo, el protocolo de calidad NFIQ seleccionado para el SBA, exige una calidad de nivel 1 o 2, siendo estos los más elevados, mientras que en el caso de que se capturen huellas con menor calidad, se deberán realizar hasta tres reintentos de captura y eventualmente, capturar la imagen de huella de otros dedos hasta completar las cuatro imágenes requeridas por el SBA. No obstante, podría no estar actualizado a las versiones más recientes del NIST y en este sentido, existe una clara oportunidad de mejora.

Por fin, en relación estricta con el almacenamiento de datos biométricos, se quiere destacar cuáles son las situaciones de mayor riesgo, las cuales también y en la medida que se mitigue ese riesgo, conllevan una clara oportunidad de mejora.

El primero y principal de los riesgos, es que los datos estén insuficientemente disociados en el almacenamiento y que una intrusión o acceso indebido a la base de datos pueda provocar un estrago masivo y mayúsculo al revelar la identidad de los datos biométricos de miles o cientos de miles de personas, a la vez que inutilizándolos como tales de ahí en más.

En la investigación realizada en relación con las medidas de seguridad del almacenamiento de los datos biométricos en ANSES no se ha podido concluir con certeza que exista alguna práctica de disociación. Por el contrario, en apariencia, los datos de identidad, tipo y número de documento, nombre y apellido, CUIL, e inclusive los llamados metadatos que no son otra cosa que el domicilio completo del beneficiario y su dirección de correo electrónico, se almacenan en la base de imágenes, la cual está vinculada de un modo directo a la base de plantillas de minucias.

Cabe señalar que la gravedad del riesgo aumenta cuanto mayor volumen o masividad tenga la base de datos biométricos y la base de datos de ANSES es una de las más voluminosas, pero de ninguna manera es la única ni la más grande del país. La del Registro Nacional de las Personas y la de Policía Federal, seguramente la superan en tamaño.

La segunda situación de riesgo, de menor alcance e impacto, pero quizás de ocurrencia mucho más probable que la descripta en los párrafos anteriores, es que cualquiera de las bases parciales u obtenidas por copia de Mi Huella puedan estar en riesgo por el mismo motivo, disminuidas por razones obvias en cantidad de casos afectados, pero multiplicadas, de la misma manera, las ocasiones de fallo por la cantidad de bases distribuidas.

Como procedimiento de contingencia, ANSES señala un almacenamiento temporal de las huellas capturadas y que se utilizará un proceso batch (por lote de transacciones) para realizar la transferencia de la información. También está

previsto que, a requerimiento de una entidad bancaria, ANSES provea una copia de las minucias de las huellas de los beneficiarios enrolados en dicha entidad.

Si se agrega a las dos situaciones anteriores que no hay ningún tipo de norma de procedimiento, guía o protocolo que indique qué hacer con los datos biométricos capturados una vez transmitidos a la base centralizada de ANSES, es posible concluir que dicha base coexiste con múltiples bases parciales de datos biométricos de los beneficiarios en cada entidad bancaria que están en su cápita. Por otra parte, refuerza la presunción de la coexistencia de bases, el imperativo de que las entidades deben estar preparadas para dar respuesta a los beneficiarios a los que pagan, aún en caso de inconexión o salidas de servicio de la plataforma de ANSES.

Luego de todo lo dicho, las recomendaciones que este trabajo argumenta para mejorar las condiciones de almacenamiento de los datos biométricos, sobre todo en bases de datos de gran volumen y orientadas a la verificación de identidad, como la del SBA y la gran mayoría de ellas, son las siguientes:

Es necesario y es posible desde el punto de vista tecnológico instrumentar medidas efectivas de anonimización entre los datos biométricos de las personas y el resto de sus datos personales.

Es conveniente que dicha instrumentación sea exigida desde las propias normas que regulan la protección de los datos personales. Si bien se ha perdido la oportunidad de un proyecto de ley con estado parlamentario, el momento sigue siendo propicio para aprovechar los antecedentes inmediatos de esta iniciativa.

Una función de hashing es probablemente la más adecuada desde el punto de vista técnico, así como económica en su implementación, para vincular en un único sentido los datos personales del titular (nombre y apellido, documentos y claves de identidad) con sus datos biométricos (imágenes o plantillas de minucias, en el caso de las huellas dactilares).

Esta instrumentación también requerirá que las bases de datos biométricos puros residan en ambientes físicos y lógicos diferentes de los propios de las bases de datos personales alfanuméricos.

También es necesario avanzar en la normativa de protección de datos personales, probablemente desde las reglamentaciones y normas de

procedimiento emitidas por la AAIP, abordando la cuestión de la conservación de los datos biométricos y estipulando plazos de guarda ciertos, limitados por condiciones o eventos fácilmente reconocibles.

Asimismo, desde las reglamentaciones y normas de procedimiento emitidas por la AAIP, es necesario estipular quiénes serán depositarios de bases de datos biométricos secundarias o de resguardo ante contingencias y bajo qué condiciones y con cuáles responsabilidades se dará esa guarda.

5.3. Próximos pasos

Seguidamente, como punto final del presente capítulo y del trabajo en su parte sustantiva, se enumeran una serie de acciones que podrían instrumentarse en un futuro cercano, a los efectos de consolidar o ampliar las mejoras propuestas:

- Investigar las funciones de hashing más adecuadas para brindar una gama de soluciones técnicas de acuerdo al volumen de la base de datos biométricos, considerando sus costos y los tiempos de procesamiento asociados, así como las alternativas de arquitectura de las soluciones y los requerimientos para su implementación.
- Brindar una propuesta de los textos a incorporar a las normas (ley de PDP, decreto reglamentario y normas complementarias o resoluciones de AAIP) a los efectos de que la anonimización adquiera fuerza legal.
- Proponer también los textos que serán incorporados en las resoluciones de la AAIP en relación con las previsiones respecto de los plazos de guarda de los datos biométricos y de las bases copia de resguardo ante contingencias.
- Diseñar un modelo del registro de auditoría de acceso a datos biométricos, a los efectos de que pueda integrarse al sistema de registro y seguimiento de incidentes proyectado por el nuevo ordenamiento legal.

GLOSARIO

Acceso: utilización de los recursos de un sistema de información.

Acceso remoto: la habilidad para acceder a una computadora desde una ubicación apartada.

Activo de información: es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones

Almacenamiento de datos: Uno de los tratamientos que pueden recibir los datos.

Anonimizar, anonimización de datos personales: Expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad.

Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Bases de datos: una gran cantidad de información que ha sido sistematizada para su correcto almacenamiento, de forma tal que los datos que allí están contenidos puedan ser utilizados cuando se considere necesario, pudiendo ser posteriormente reordenados u organizados.

Big data: en español, grandes datos o grandes volúmenes de datos) es un término que describe cualquier cantidad voluminosa de datos estructurados, semiestructurados y no estructurados que tienen el potencial de ser extraídos o tratados para obtener información.

Biometría: Es la ciencia y la tecnología dedicadas a medir y analizar datos biológicos. En el terreno de la informática, la biometría hace referencia a las tecnologías que miden y analizan las características del cuerpo humano, como el ADN, las huellas dactilares, la retina y el iris de los ojos, los patrones faciales o de la voz, entre otros, a efectos de identificar personas.

Cifrado: proceso para convertir información en un formato ilegible aplicando un algoritmo criptográfico que se utiliza para proteger la información de la divulgación no autorizada. Sinónimo de algoritmo de cifra.

Datos biométricos: datos personales referidos a las características físicas, fisiológicas o conductuales de una persona que posibiliten o aseguren su identificación única. Por ejemplo imágenes faciales o huellas dactilares.

Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Hash (código): bits obtenidos como resultado de aplicar una función resumen o de una sola vía a unos datos.

Incidente: una ocurrencia que real o potencialmente resulte en una consecuencia adversa o amenaza para un sistema de información o la información que el sistema procesa, almacena o transmite.

Incidente de seguridad: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa u organismo.

Información pública: todo tipo de dato contenido en documentos de cualquier formato que los sujetos obligados por la Ley de AIP generen, obtengan, transformen, controlen o custodien.

Nube, computación en la nube: modelo de trabajo que permite ofrecer servicios de computación a través de una red que usualmente es Internet. Permite almacenar información, ficheros y datos en servidores de terceros de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red.

Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

Riesgos, análisis de riesgos: es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan en general la recolección, conservación y el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

Vulnerabilidad: debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

APÉNDICES – ANEXO I

Marco normativo: principales leyes y decretos

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo I Disposiciones Generales. Artículos 1 Objeto y 2 Definiciones	**Objeto: la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información** que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. **Define:** • Datos personales. • Datos sensibles. • Archivo, registro, base o banco de datos, indistintamente. • Tratamiento de datos. • Responsable de archivo, registro, base o banco de datos. • Datos informatizados. • Titular de los datos. • Usuario de datos. • **Disociación de datos.**
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo II Principios generales relativos a la protección de datos Art. 3 Licitud, Art. 4 Calidad de los datos, Art. 5 Consentimiento, Art. 6 Información	**La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos.** Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo, sin perjuicio de los derechos del titular. **Deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.** Deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6°. Entre otras situaciones, no será necesario el consentimiento cuando los datos se obtengan de fuentes de acceso público irrestricto o se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio (básicamente padrón electoral o cuil) Cuando se recaben datos personales se deberá informar previamente a sus titulares la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios, así como la identificación del archivo, registro o banco de datos, entre otras cuestiones.
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo II **Principios** continuación. Art 7 Categorías de datos, Art. 8 Datos sobre salud; Art. 9 Seguridad de los datos.	Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de sus pacientes respetando los principios del secreto profesional. **El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado. Por lo que está prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.**
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo II Principios continuación. Art. 10 Deber de confidencialidad, Art. **11 Cesión**, Art 12 Transferencia internacional	Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento expreso del titular de los datos. Puede revocarse. Generalmente, el consentimiento no es exigido cuando: • Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; • **Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.**

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados. La prohibición no regirá ante: • Colaboración judicial internacional; • Intercambio de datos necesarios por razones de salud pública y siempre que se protejan con procedimientos de disociación. • Transferencias bancarias o bursátiles, conforme la legislación aplicable. • En el marco de tratados internacionales. • Por cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo III Derechos de los titulares de los datos. Art. 13 Derecho de información, Art. 14 Derecho de acceso, Art. 15. Contenido de la información. Art. 16 Derecho de rectificación, actualización o supresión.	Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita. **El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados.** El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente, vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley. **Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.** El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado en el plazo máximo de cinco días hábiles.
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo III Derechos de los titulares de datos - continuación. Art. 17 Excepciones,	Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. O si se pudieran obstaculizar actuaciones judiciales o

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
			Art. 18 Comisiones legislativas, Art. 19 Gratuidad, Art 20 Impugnación de valoraciones personales.	administrativas o investigaciones en curso. Las Comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a determinados archivos o bancos de datos por razones fundadas o de su competencia. La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo IV Usuarios y responsables de archivos, registros y bancos de datos. Art 21 Registro de archivos. Inscripción; Art. 22 **Archivos**, registros o bancos de datos públicos.	Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control. a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) Forma de recolección y actualización de datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; **f) Modo de interrelacionar la información registrada;** **g) Medios utilizados para garantizar la seguridad de los datos**; h) Tiempo de conservación de los datos; i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos. **Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial.** **Las disposiciones respectivas, deben indicar: características y finalidad del archivo; personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas; procedimiento de obtención y actualización de los datos y estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán; entre otros.**
1	**Ley N° 25.326**	Octubre de	Capítulo IV Usuarios y	Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
	Protección de Datos Personales	2000	responsables de archivos, registros y bancos de datos. Art 23 Supuestos especiales, 24 Archivos, registros o bancos de datos privados; Art 25 Prestación de servicios informatizados de datos personales; Art. 26 Prestación de servicios de información crediticia. Art 27 Archivos con fines de publicidad; Art 28 Archivos relativos a encuestas.	almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. **Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.** **Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna**.
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo V Control – Art. 29 Órgano de control, Art. 30 códigos de conducta	El órgano de control tendrá las siguientes funciones y atribuciones: a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley; c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos; d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley; e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados; f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia; g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley; h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley. Códigos de conducta: 1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley. 2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo VI Sanciones. Art. 31 Sanciones administrativas; Art. 32 Sanciones penales	El organismo de control podrá aplicar las sanciones administrativas de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos. La reglamentación determinará las condiciones y procedimientos para su aplicación. En relación con sanciones penales, se incorpora como artículo 117 bis del Código Penal,

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				el siguiente: "1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales. 2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales. 3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona. 4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena". Como artículo 157 bis del Código Penal el siguiente: "Será reprimido con la pena de prisión de un mes a dos años el que: 1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. 3° Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	**Capítulo VII Acciones de protección de los datos personales.** Art. 33 Procedencia; Art. 34 Legitimación Activa; Art. 35 Legitimación Pasiva; Art. 36 Competencia; Art. 37 Procedimiento Aplicable; Art. 38 Requisitos de la demanda; Art. 39 Trámite	La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización. **Legitimación activa:** La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. **En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.** **Legitimación pasiva:** La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes. Será competente para entender en esta acción el juez del domicilio del actor; el del

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Procederá la competencia federal cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales. **La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo**…. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Capítulo VII Acciones de protección de los datos personales. Art. 40 Confidencialidad de la información; Art. 41 Contestación del informe; Art. 42 Ampliación de la demanda; Art. 43 Sentencia	Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad. Al contestar el informe, el banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley. Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días.

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto.
1	**Ley N° 25.326 Protección de Datos Personales**	Octubre de 2000	Art 44 AMBITO DE APLICACIÓN	Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional. Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.
2	**Decreto 1558/2001 Aprueba la reglamentación de la Ley Nº 25.326.**	Noviembre de 2001	**Principios generales relativos a la protección de datos. Capítulos I y II de la Ley**	**Se invita a las Provincias y a la CIUDAD AUTONOMA DE BUENOS AIRES a adherir a las normas de exclusiva aplicación nacional de esta reglamentación.** A los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito. El dato que hubiera perdido vigencia respecto de los fines para los que se hubiese obtenido o recolectado debe ser suprimido por el responsable o usuario sin necesidad de que lo requiera el titular de los datos. La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES efectuará controles de oficio sobre el cumplimiento de este principio legal, y aplicará las sanciones pertinentes al responsable o usuario en los casos que correspondiere. La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES procederá, ante el pedido de un interesado o de oficio ante la sospecha de una ilegalidad, a verificar

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				el cumplimiento de las disposiciones legales y reglamentarias ARTICULO 5º.- El consentimiento informado es el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el artículo 6º de la Ley Nº 25.326. La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES establecerá los requisitos para que el consentimiento pueda ser prestado por un medio distinto a la forma escrita, el cual deberá asegurar la autoría e integridad de la declaración. El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo. La revocación no tiene efectos retroactivos. ARTICULO 12.- La prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión. Facúltase a la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional.
2	**Decreto 1558/2001 Aprueba la reglamentación de la Ley Nº 25.326.**	Noviembre de 2001	**Derechos de los titulares de los datos.**	ARTICULO 14.- La solicitud a que se refiere el artículo 14, inciso 1, de la Ley Nº 25.326, no requiere de fórmulas específicas, siempre que garantice la identificación del titular. Se puede efectuar de manera directa, presentándose el interesado ante el responsable o usuario del archivo, registro, base o banco de datos, o de manera indirecta, a través de la intimación fehaciente por medio escrito que deje constancia de recepción. También pueden ser utilizados otros servicios de acceso directo o semidirecto como los medios electrónicos, las líneas telefónicas, etc. El derecho de acceso permitirá: a) conocer si el titular de los datos se encuentra o no en el archivo, registro, base o banco de datos; b) conocer todos los datos relativos a su persona que constan en el archivo; c) solicitar información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos; d) solicitar las finalidades para las que se recabaron; e) conocer el destino previsto para los datos personales; f) saber si el archivo está registrado conforme a las exigencias de la Ley Nº 25.326.

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				ARTICULO 16.- En las disposiciones de los artículos 16 a 22 y 38 a 43 de la Ley Nº 25.326 en que se menciona a algunos de los derechos de rectificación, actualización, supresión y confidencialidad, se entiende que tales normas se refieren a todos ellos.
2	**Decreto 1558/2001 Aprueba la reglamentación de la Ley Nº 25.326.**	Noviembre de 2001	***Aplicaría al caso Mi Huella***	En el caso de los archivos o bases de datos públicas conformadas por cesión de información suministrada por entidades financieras, administradoras de fondos de jubilaciones y pensiones y entidades aseguradoras, de conformidad con el artículo 5º, inciso 2, de la Ley Nº 25.326, los derechos de rectificación, actualización, supresión y confidencialidad deben ejercerse ante la entidad cedente que sea parte en la relación jurídica a que se refiere el dato impugnado. Si procediera el reclamo, la entidad respectiva debe solicitar al BANCO CENTRAL DE LA REPUBLICA ARGENTINA, a la SUPERINTENDENCIA DE ADMINISTRADORAS DE FONDOS DE JUBILACIONES Y PENSIONES o a la SUPERINTENDENCIA DE SEGUROS DE LA NACION, según el caso, que sean practicadas las modificaciones necesarias en sus bases de datos. Toda modificación debe ser comunicada a través de los mismos medios empleados para la divulgación de la información.
2	**Decreto 1558/2001 Aprueba la reglamentación de la Ley Nº 25.326.**	Noviembre de 2001	**Usuarios y responsables de archivos, registros y bancos de datos.**	ARTICULO 25.- Los contratos de prestación de servicios de tratamiento de datos personales deberán contener los niveles de seguridad previstos en la Ley Nº 25.326, esta reglamentación y las normas complementarias que dicte la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, como así también las obligaciones que surgen para los locatarios en orden a la confidencialidad y reserva que deben mantener sobre la información obtenida. La realización de tratamientos por encargo deberá estar regulada por un contrato que vincule al encargado del tratamiento con el responsable o usuario del tratamiento.
2	**Decreto 1558/2001 Aprueba la reglamentación de la Ley Nº 25.326.**	Noviembre de 2001	**Control. Sanciones.**	ARTICULO 29. La AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, conforme los términos del artículo 19 de la Ley N° 27.275, sustituido por el artículo 11 del Decreto N° 746/17, es el órgano de control de la Ley Nº 25.326. (Artículo sustituido por art. 1° del Decreto N° 899/2017 B.O. 6/11/2017) ARTÍCULO 30.- La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES alentará la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				disposiciones nacionales adoptadas por la Ley Nº 25.326 y esta reglamentación.
3	**Decreto 1160/2010 Modifica el Anexo I del Decreto Nº 1558/01.**	Agosto de 2010	**Art. Único.** Sustituye el inciso 3 del artículo 31 del Anexo I del Decreto Nº 1558/01 relativo al procedimiento a seguir para la aplicación de sanciones.	Se sustituye el inciso 3. del artículo 31 del Anexo I del Decreto Nº 1558/01 por el siguiente: "3. El procedimiento se ajustará a las siguientes disposiciones: a) La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES (DNPDP) iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones de la Ley Nº 25.326, sus normas reglamentarias y complementarias, de oficio o por denuncia de quien invocare un interés particular, del Defensor del Pueblo de la Nación o de asociaciones de consumidores o usuarios. b) Para el cumplimiento de sus cometidos, la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES podrá realizar múltiples acciones: I) Comprobar la legitimidad de todas las operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias. III) Verificar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. IV) Velar por el cumplimiento de los plazos establecidos en los artículos 14 y 16 de la Ley Nº 25.326 para el ejercicio de los derechos de acceso, rectificación, supresión, actualización y confidencialidad reconocidos a los titulares de datos personales. V) Realizar investigaciones e inspecciones. VI) Solicitar la presentación de informes a los responsables de bancos de datos y de su tratamiento. VII) Formular requerimientos ante las autoridades nacionales, provinciales y municipales. VIII) Realizar inspecciones. IX) Solicitar al juez competente el auxilio de la fuerza pública para realizar el allanamiento de domicilios; la Clausura de registros; el secuestro de documentación y toda otra medida tendiente al cabal cumplimiento de la actividad investigativa. c) Para el inicio del procedimiento, el denunciante deberá presentar ante la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES un escrito, el que deberá contener fecha, firma y aclaración; documento de identidad (DNI-CUIL-CUIT), domicilio, la relación del hecho denunciado con las circunstancias de lugar, tiempo y modo de ejecución y demás elementos que puedan conducir a su comprobación, como mínimo.

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				Deberá acompañar en el mismo acto la documentación y antecedentes que confirmen sus dichos y acreditar en el momento de la interposición de la denuncia, las gestiones previas ante el responsable de la base de datos, cuando se tratare de cuestiones referidas a los derechos de acceso, actualización, rectificación, supresión, confidencialidad o bloqueo, regulados en los artículos 14, 16 y 27 de la Ley Nº 25.326. Se iniciará un proceso de instrucción o investigación de la presunta infracción y se dictará resolución que deberá ser notificada al infractor. Contra la resolución definitiva procederá la vía recursiva prevista en el REGLAMENTO DE PROCEDIMIENTOS ADMINISTRATIVOS (Decreto Nº 1759/72 - t.o. 1991) y sus modificatorios. Dictada la resolución que impone una sanción administrativa, la constancia de la misma deberá ser incorporada en el REGISTRO DE INFRACTORES LEY Nº 25.326, que lleva la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES. Las constancias de dicho Registro relativas a aquellas sanciones aplicadas que se encuentren firmes deberán publicarse en el sitio de Internet de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES (www.jus.gov.ar/dnpdpnew).
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título preliminar: Artículo 1 Objeto, Principios,	**La presente ley tiene por objeto garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover la participación ciudadana y la transparencia de la gestión pública**, y se funda en los siguientes principios: **Presunción de publicidad**: toda la información en poder del Estado se presume pública, salvo las excepciones previstas por esta ley. **Transparencia y máxima divulgación**: toda la información en poder, custodia o bajo control del sujeto obligado debe ser accesible para todas las personas. El acceso a la información pública sólo puede ser limitado cuando concurra alguna de las excepciones previstas en esta ley, de acuerdo con las necesidades de la sociedad democrática y republicana, proporcionales al interés que las justifican. **Informalismo**: las reglas de procedimiento para acceder a la información deben facilitar el ejercicio del derecho. Los sujetos obligados no pueden fundar el rechazo de la solicitud de información en el incumplimiento de requisitos formales o de reglas de procedimiento. **Máximo acceso**: la información debe publicarse de forma completa, con el mayor nivel de desagregación posible y por la mayor cantidad de medios disponibles. **Apertura**: la información debe ser accesible en formatos electrónicos abiertos, que faciliten su procesamiento por medios automáticos que permitan su reutilización o su

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				redistribución por parte de terceros. **Disociación**: en aquel caso en el que parte de la información se encuadre dentro de las excepciones taxativamente establecidas por esta ley, la información no exceptuada debe ser publicada en una versión del documento que tache, oculte o disocie aquellas partes sujetas a la excepción. **No discriminación**: se debe entregar información a todas las personas que lo soliciten. **Máxima premura**: la información debe ser publicada con la máxima celeridad y en tiempos compatibles con la preservación de su valor. **Gratuidad**: el acceso a la información debe ser gratuito, sin perjuicio de lo dispuesto en esta ley. **Control**: el cumplimiento de las normas que regulan el derecho de acceso a la información será objeto de fiscalización permanente. Las resoluciones que denieguen solicitudes de acceso a la información, como el silencio del sujeto obligado requerido, la ambigüedad o la inexactitud de su repuesta, podrán ser recurridas ante el órgano competente. **Responsabilidad**: el incumplimiento de las obligaciones que esta ley impone originará responsabilidades y dará lugar a las sanciones que correspondan. **Alcance limitado de las excepciones**: los límites al derecho de acceso a la información pública deben ser excepcionales, establecidos previamente conforme a lo estipulado en esta ley, y formulados en términos claros y precisos, quedando la responsabilidad de demostrar la validez de cualquier restricción al acceso a la información a cargo del sujeto al que se le requiere la información. **In dubio pro petitor**: la interpretación de las disposiciones de esta ley o de cualquier reglamentación del derecho de acceso a la información debe ser efectuada, en caso de duda, siempre en favor de la mayor vigencia y alcance del derecho a la información. **Facilitación**: ninguna autoridad pública puede negarse a indicar si un documento obra, o no, en su poder o negar la divulgación de un documento de conformidad con las excepciones contenidas en la presente ley, salvo que el daño causado al interés protegido sea mayor al interés público de obtener la información. **Buena fe**: para garantizar el efectivo ejercicio del acceso a la información, resulta esencial que los sujetos obligados actúen de buena fe.
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título I Derecho de acceso a la Información Pública. Capítulo I Régimen General. Art 2	**El derecho de acceso a la información pública comprende la posibilidad de buscar, acceder, solicitar, recibir, copiar, analizar, reprocesar, reutilizar y redistribuir libremente la información bajo custodia de los sujetos obligados enumerados en el artículo 7° de la presente ley, con las únicas limitaciones y excepciones que establece esta norma.**

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
			Derecho de acceso a la información pública; Art. 3 Definiciones; Art. 4 Legitimación Activa; Art. 5 Entrega de la información; Art. 6 Gratuidad	**Se presume pública toda información que generen, obtengan, transformen, controlen o custodien los sujetos obligados alcanzados por esta ley.** A los fines de la presente ley se entiende por: **Información pública: todo tipo de dato contenido en documentos de cualquier formato que los sujetos obligados enumerados en el artículo 7° de la presente ley generen, obtengan, transformen, controlen o custodien;** **Documento: todo registro que haya sido generado, que sea controlado o que sea custodiado por los sujetos obligados enumerados en el artículo 7° de la presente ley, independientemente de su forma, soporte, origen, fecha de creación o carácter oficial.** Toda persona humana o jurídica, pública o privada, tiene derecho a solicitar y recibir información pública, no pudiendo exigirse al solicitante que motive la solicitud, que acredite derecho subjetivo o interés legítimo o que cuente con patrocinio letrado. La información debe ser brindada en el estado en el que se encuentre al momento de efectuarse la solicitud, no estando obligado el sujeto requerido a procesarla o clasificarla. El Estado tiene la obligación de entregarla en formatos digitales abiertos, salvo casos excepcionales en que fuera de imposible cumplimiento o significara un esfuerzo estatal desmedido. Las excepciones las fijará la Agencia de Acceso a la Información Pública. El acceso a la información pública es gratuito en tanto no se requiera su reproducción. Los costos de reproducción corren a cargo del solicitante.
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título I Derecho de acceso a la Información Pública. Capítulo I Régimen General. Art. 7 AMBITO DE APLICACIÓN	Son sujetos obligados a brindar información pública: • La administración pública nacional, conformada por la administración central y los organismos descentralizados, comprendiendo en estos últimos a las instituciones de seguridad social; • El Poder Legislativo y los órganos que funcionan en su ámbito; • El Poder Judicial de la Nación; • El Ministerio Público Fiscal de la Nación;

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				• El Ministerio Público de la Defensa; • El Consejo de la Magistratura; • Las empresas y sociedades del Estado, sólo en lo referido a la participación estatal; • Concesionarios, permisionarios y licenciatarios de servicios públicos o concesionarios permisionarios de uso del dominio público, en la medida en que cumplan servicios públicos; • Organizaciones empresariales, partidos políticos, sindicatos, universidades y cualquier entidad privada a la que se le hayan otorgado fondos públicos, en lo que se refiera, únicamente, a la información producida total o parcialmente o relacionada con los fondos públicos recibidos; • Instituciones o fondos cuya administración, guarda o conservación esté a cargo del Estado nacional; • Personas jurídicas públicas no estatales en todo aquello que estuviese regulado por el derecho público; • Fideicomisos que se constituyeren total o parcialmente con recursos o bienes del Estado nacional; • Los entes cooperadores con los que la administración pública nacional hubiera celebrado o celebre • El Banco Central de la República Argentina; • Los entes interjurisdiccionales en los que el Estado nacional tenga participación o representación; • Los concesionarios, explotadores, administradores y operadores de juegos de azar, destreza y apuesta, debidamente autorizados por autoridad competente. **El incumplimiento de la presente ley será considerado causal de mal desempeño.**
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título I Derecho de acceso a la Información Pública. Capítulo II **Excepciones. Art. 8 Excepciones**	Los sujetos obligados sólo podrán exceptuarse de proveer la información cuando se configure alguno de los siguientes supuestos: a) Información expresamente clasificada como reservada o confidencial o secreta, por razones de defensa o política exterior. b) Información que pudiera poner en peligro el correcto funcionamiento del sistema financiero o bancario; c) Secretos industriales, comerciales, financieros, científicos, técnicos o tecnológicos cuya revelación pudiera perjudicar el nivel de competitividad o lesionar los intereses del sujeto obligado;

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				d) Información que comprometa los derechos o intereses legítimos de un tercero obtenida en carácter confidencial; e) Información en poder de la Unidad de Información Financiera encargada del análisis, tratamiento y transmisión de información tendiente a la prevención e investigación de la legitimación de activos provenientes de ilícitos; f) Información elaborada por los sujetos obligados dedicados a regular o supervisar instituciones financieras o preparada por terceros para ser utilizada por aquellos y que se refieran a exámenes de situación, evaluación de su sistema de operación o condición de su funcionamiento; g) Información elaborada por asesores jurídicos o abogados de la administración pública nacional cuya publicidad pudiera revelar la estrategia a adaptarse en la defensa o tramitación de una causa judicial o divulgare las técnicas o procedimientos de investigación de algún delito u otra irregularidad o cuando la información privare a una persona del pleno ejercicio de la garantía del debido proceso; h) Información protegida por el secreto profesional; **i) Información que contenga datos personales y no pueda brindarse aplicando procedimientos de disociación, salvo que se cumpla con las condiciones de licitud previstas en la ley 25.326 de protección de datos personales y sus modificatorias;** j) Información que pueda ocasionar un peligro a la vida o seguridad de una persona; k) Información de carácter judicial cuya divulgación estuviera vedada por otras leyes o por compromisos contraídos por la República Argentina en tratados internacionales; l) Información obtenida en investigaciones realizadas por los sujetos obligados que tuviera el carácter de reservada y cuya divulgación pudiera frustrar el éxito de una investigación; m) Información correspondiente a una sociedad anónima sujeta al régimen de oferta pública. Las excepciones contenidas en el presente artículo no serán aplicables en casos de graves violaciones de derechos humanos, genocidio, crímenes de guerra o delitos de lesa humanidad.
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título I Derecho de acceso a la Información Pública. Capítulo III Solicitud de información y vías de reclamo. Art. 9 Solicitud de	La solicitud de información debe ser presentada ante el sujeto obligado que la posea o se presuma que la posee, quien la remitirá al responsable de acceso a la información pública, en los términos de lo previsto en el artículo 30 de la presente ley. Si la solicitud se refiere a información pública que no obre en poder del sujeto al que se dirige, éste la remitirá, dentro del plazo improrrogable de cinco (5) días, computado desde la presentación, a quien la posea, si lo conociera, o en caso contrario a la Agencia de Acceso a la Información Pública.

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
			información; Art. 10 Tramitación; Art. 11 Plazos; Art. 12 Información parcial; Art. 13 Denegatoria	**Toda solicitud de información pública requerida en los términos de la presente ley debe ser satisfecha en un plazo no mayor de quince (15) días hábiles. El plazo se podrá prorrogar en forma excepcional por otros quince (15) días hábiles.** Los sujetos obligados deben brindar la información solicitada en forma completa. Cuando exista un documento que contenga en forma parcial información cuyo acceso esté limitado en los términos del artículo 8° de la presente ley, deberá suministrarse el resto de la información solicitada, utilizando sistemas de tachas.
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título I Derecho de acceso a la Información Pública. Capítulo III Solicitud de información y vías de reclamo. Art. 13 Denegatoria; Art. 14 Vías de reclamo; Art. 15 Reclamo por incumplimiento. Art.16 Requisitos formales.	El sujeto requerido sólo podrá negarse a brindar la información objeto de la solicitud, por acto fundado, si se verificara que la misma no existe y que no está obligado legalmente a producirla o que está incluida dentro de alguna de las excepciones previstas en el artículo 8° de la presente ley. La falta de fundamentación determinará la nulidad del acto denegatorio y obligará a la entrega de la información requerida. La denegatoria de la información debe ser dispuesta por la máxima autoridad del organismo o entidad requerida. El silencio del sujeto obligado, vencidos los plazos previstos en el artículo 11 de la presente ley, así como la ambigüedad, inexactitud o entrega incompleta, serán considerados como denegatoria injustificada a brindar la información. Las decisiones en materia de acceso a la información pública son recurribles directamente ante los tribunales de primera instancia en lo contencioso administrativo federal, sin perjuicio de la posibilidad de interponer el reclamo administrativo pertinente ante la Agencia de Acceso a la Información Pública o el órgano que corresponda según el legitimado pasivo. Será competente el juez del domicilio del requirente o el del domicilio del ente requerido, a opción del primero. En ninguno de estos dos supuestos, podrá ser exigido el agotamiento de la vía administrativa. El reclamo por incumplimiento previsto en el artículo 15 de la presente ley, será sustitutivo de los recursos previstos en la Ley Nacional de Procedimientos Administrativos, 19.549, y en el decreto 1.759 del 3 de abril de 1972 (t.o. 1991). El reclamo promovido mediante acción judicial tramitará por la vía del amparo y deberá ser interpuesto dentro de los cuarenta (40) días hábiles desde que fuera notificada la resolución denegatoria de la solicitud o desde que venciera el plazo para responderla.

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				Ante los supuestos de denegatoria de una solicitud de información establecidos en el artículo 13 de la presente ley o ante cualquier otro incumplimiento a lo dispuesto en la presente, el solicitante podrá, dentro de un plazo de cuarenta (40) días hábiles interponer un reclamo ante la Agencia de Acceso a la Información Pública o, a su opción, ante el organismo originalmente requerido. Este último deberá elevarlo de inmediato y sin dilación a la Agencia de Acceso a la Información Pública para su resolución.
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título I Derecho de acceso a la Información Pública. Capítulo III Solicitud de información y vías de reclamo. Art.17 Resolución del reclamo interpuesto; Art. 18 Responsabilidades	Dentro de los treinta (30) días hábiles contados desde la recepción del reclamo por incumplimiento, la Agencia de Acceso a la Información Pública, deberá decidir si a) rechazar fundadamente el reclamo, siendo motivos para dicha resolución: I. Que se hubiese presentado fuera del plazo previsto; II. Que con anterioridad hubiera resuelto la misma cuestión en relación al mismo requirente y a la misma información; III. Que el sujeto requerido no sea un sujeto obligado por la presente ley; IV. Que se trate de información contemplada en alguna o algunas de las excepciones establecidas en el artículo 8° de la presente ley. V. Que la información proporcionada haya sido completa y suficiente. O b) Intimar al sujeto obligado que haya denegado la información requerida a cumplir con las obligaciones que le impone esta ley, el que deberá entregar la información solicitada en un plazo no mayor a diez (10) días hábiles desde recibida la intimación. Responsabilidades. El funcionario público o agente responsable que en forma arbitraria obstruya el acceso del solicitante a la información pública requerida, o la suministre en forma incompleta u obstaculice de cualquier modo el cumplimiento de esta ley, incurre en falta grave sin perjuicio de las responsabilidades administrativas, patrimoniales y penales que pudieran caberle conforme lo previsto en las normas vigentes.
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título I Derecho de acceso a la Información Pública. Capítulo IV Agencia de Acceso a la Información Pública. Art 19 Creación; Art.	Créase la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, como ente autárquico que funcionará con autonomía funcional en el ámbito de la JEFATURA DE GABINETE DE MINISTROS. La AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA debe velar por el cumplimiento de los principios y procedimientos establecidos en la presente ley, garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover medidas de transparencia activa y actuar como Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326.

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
			20 Director de la AAIP; Art. 21 Procedimiento de selección del director; Art. 22 Rango y jerarquía del director; Art. 23 Requisitos e incompatibilidades	La Agencia de Acceso a la Información Pública estará a cargo de un director que durará cinco (5) años en el cargo con posibilidad de ser reelegido por una única vez. El director será designado por el Poder Ejecutivo nacional mediante un procedimiento de selección público, abierto y transparente que garantice la idoneidad del candidato. El director a cargo de la Agencia de Acceso a la Información Pública tendrá rango y jerarquía de secretario. El ejercicio de la función requiere dedicación exclusiva y resulta incompatible con cualquier otra actividad pública o privada, excepto la docencia a tiempo parcial. Está vedada cualquier actividad partidaria mientras dure el ejercicio de la función. Ningún funcionario a cargo de la Agencia de Acceso a la Información Pública podrá tener intereses o vínculos con los asuntos bajo su órbita en las condiciones establecidas por la Ley de Ética en el Ejercicio de la Función Pública, 25.188, sus modificaciones y su reglamentación.
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título I Derecho de acceso a la Información Pública. **Capítulo IV Agencia de Acceso a la Información Pública. Art 24 Competencias y funciones;** Art. 25 Personal de la AAIP; Art. 26 Cese del director de la AAIP; Art. 27 Remoción del director de la AAIP; Art. 28 Organismos de acceso a la información pública en Poder Legislativo, Poder Judicial y Ministerios Públicos. Art. 29 Consejo Federal de la	Son competencias y funciones de la Agencia de Acceso a la Información Pública, entre otras las siguientes: • Redactar y aprobar el Reglamento de Acceso a la Información Pública aplicable a todos los sujetos obligados; • Implementar una plataforma tecnológica para la gestión de las solicitudes de información y sus correspondientes respuestas; • Requerir a los sujetos obligados que modifiquen o adecuen su organización, procedimientos, sistemas de atención al público y recepción de correspondencia a la normativa aplicable a los fines de cumplir con el objeto de la presente ley; • Elaborar criterios orientadores e indicadores de mejores prácticas destinados a los sujetos obligados; • Elaborar y presentar ante el Honorable Congreso de la Nación propuestas de reforma legislativa respecto de su área de competencia; • Solicitar a los sujetos obligados expedientes, informes, documentos, antecedentes y cualquier otro elemento necesario a los efectos de ejercer su labor; • Recibir y resolver los reclamos administrativos que interpongan los solicitantes de información pública según lo establecido por la presente ley respecto de todos los obligados, con excepción de los previstos en los incisos b) al f) del artículo 7° de la presente, y publicar las resoluciones que se dicten en ese

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
			Transparencia.	marco; • Promover las acciones judiciales que correspondan, para lo cual la Agencia de Acceso a la Información Pública tiene legitimación procesal activa en el marco de su competencia; • Impulsar las sanciones administrativas pertinentes ante las autoridades competentes correspondientes en los casos de incumplimiento a lo establecido en la presente ley; • Publicar los índices de información reservada elaborados por los sujetos obligados. En un plazo máximo de noventa (90) días contado desde la publicación de la presente ley en el Boletín Oficial, el Poder Legislativo, el Poder Judicial de la Nación, el Ministerio Público Fiscal de la Nación, el Ministerio Público de la Defensa y el Consejo de la Magistratura crearán, cada uno de ellos, un organismo con autonomía funcional y con competencias y funciones idénticas a las de la Agencia de Acceso a la Información Pública previstas en el artículo 24 de la presente ley, que actuará en el ámbito del organismo en el que se crea. Créase el Consejo Federal para la Transparencia, como organismo interjurisdiccional de carácter permanente, que tendrá por objeto la cooperación técnica y la concertación de políticas en materia de transparencia y acceso a la información pública. Con sede en la AAIP, estará integrado por un (1) representante de cada una de las provincias y un (1) representante de la Ciudad Autónoma de Buenos Aires, que deberán ser los funcionarios de más alto rango en la materia de sus respectivas jurisdicciones.
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título I Derecho de acceso a la Información Pública. Capítulo V Responsables de Acceso a la Información Pública. Art. 30 Responsables; Art. 31 Funciones de los Responsables;	Cada uno de los sujetos obligados deberá nombrar a un responsable de acceso a la información pública que deberá tramitar las solicitudes de acceso a la información pública dentro de su jurisdicción. Serán funciones de los responsables de acceso a la información pública, en el ámbito de sus respectivas jurisdicciones: Recibir y dar tramitación a las solicitudes de acceso a la información pública, remitiendo la misma al funcionario pertinente; Realizar el seguimiento y control de las solicitudes; Llevar un registro de las mismas; Promover la implementación de las resoluciones elaboradas por AAIP y prácticas de transparencia en la gestión pública;

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				Publicar, en caso de corresponder, la información que hubiese sido desclasificada; Informar y mantener actualizadas a las distintas áreas de la jurisdicción correspondiente sobre la normativa vigente en materia de guarda, conservación y archivo de la información y promover prácticas en relación con dichas materias, con la publicación de la información y con el sistema de procesamiento de la información; Entre otras.
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título II Transparencia Activa. Art. 32 Transparencia activa; Art. 33 Régimen más amplio de publicidad. Art. 34 Excepciones a la transparencia activa	Los sujetos obligados enumerados en el artículo 7° de la presente ley, con excepción de los indicados en sus incisos i) y q), deberán facilitar la búsqueda y el acceso a la información pública a través de su página oficial de la red informática, de una manera clara, estructurada y entendible para los interesados y procurando remover toda barrera que obstaculice o dificulte su reutilización por parte de terceros. Asimismo, los sujetos obligados deberán publicar en forma completa, actualizada, por medios digitales y en formatos abiertos: • Un índice de la información pública que estuviese en su poder con el objeto de orientar a las personas en el ejercicio del derecho de acceso a la información pública, indicando, además, dónde y cómo deberá realizarse la solicitud; • Su estructura orgánica y funciones; • La nómina de autoridades y personal de la planta permanente y transitoria u otra modalidad de contratación, incluyendo consultores, pasantes y personal contratado en el marco de proyectos financiados por organismos multilaterales, detallando sus respectivas funciones y posición en el escalafón; • Las escalas salariales, incluyendo todos los componentes y subcomponentes del salario total, correspondientes a todas las categorías de empleados, funcionarios, consultores, pasantes y contratados; • El presupuesto asignado a cada área, programa o función, las modificaciones durante cada ejercicio anual y el estado de ejecución actualizado en forma trimestral hasta el último nivel de desagregación en que se procese; • Las transferencias de fondos provenientes o dirigidos a personas humanas o jurídicas, públicas o privadas y sus beneficiarios; • El listado de las contrataciones públicas, licitaciones, concursos, obras públicas y adquisiciones de bienes y servicios, especificando objetivos, características, montos y proveedores, así como los socios y accionistas principales, de las sociedades o empresas proveedoras; • Todo acto o resolución, de carácter general o particular, especialmente las

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				normas que establecieran beneficios para el público en general o para un sector, las actas en las que constara la deliberación de un cuerpo colegiado, la versión taquigráfica y los dictámenes jurídicos y técnicos producidos antes de la decisión y que hubiesen servido de sustento o antecedente; • Los informes de auditorías o evaluaciones, internas o externas, realizadas previamente, durante o posteriormente, referidas al propio organismo, sus programas, proyectos y actividades; • Los permisos, concesiones y autorizaciones otorgados y sus titulares; • Los servicios que brinda el organismo directamente al público, incluyendo normas, cartas y protocolos de atención al cliente; • Todo mecanismo o procedimiento por medio del cual el público pueda presentar peticiones, acceder a la información o de alguna manera participar o incidir en la formulación de la política o el ejercicio de las facultades del sujeto obligado; • Información sobre la autoridad competente para recibir las solicitudes de información pública y los procedimientos dispuestos por esta ley para interponer los reclamos ante la denegatoria; • Un índice de trámites y procedimientos que se realicen ante el organismo, así como los requisitos y criterios de asignación para acceder a las prestaciones; • Mecanismos de presentación directa de solicitudes o denuncias a disposición del público en relación a acciones u omisiones del sujeto obligado; • **Una guía que contenga información sobre sus sistemas de mantenimiento de documentos, los tipos y formas de información que obran en su poder y las categorías de información que publica;** • Las acordadas, resoluciones y sentencias que estén obligados a publicar de acuerdo con lo establecido en la ley 26.856; • La información que responda a los requerimientos de información pública realizados con mayor frecuencia; • Las declaraciones juradas de aquellos sujetos obligados a presentarlas en sus ámbitos de acción; • Cualquier otra información que sea de utilidad o se considere relevante para el ejercicio del derecho de acceso a la información pública. El acceso a todas las secciones del Boletín Oficial será libre y gratuito a través de Internet. A los fines del cumplimiento de lo previsto en el artículo 32 de la presente ley, serán de aplicación, en su caso, las excepciones al derecho de acceso a la información pública

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				previstas en el artículo 8° de esta norma y, **especialmente, la referida a la información que contenga datos personales.**
4	**Ley 27.275 Derecho de Acceso a la Información Pública**	Septiembre de 2016	Título III Disposiciones de aplicación transitoria. Art. 35 Presupuesto; Art. 36 Adhesión; Art. 37 Reglamentación; Art. 38 Cláusula transitoria 1; Art. 39 Cláusula transitoria 2; Art. 40 de forma	Invítase a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir a las disposiciones de la presente ley. El Poder Ejecutivo nacional reglamentará la presente ley dentro de los noventa (90) días desde su promulgación. Cláusula transitoria 1. Las disposiciones de la presente ley entrarán en vigencia al año de su publicación en el Boletín Oficial. Los sujetos obligados contarán con el plazo máximo de un (1) año desde la publicación de la presente ley en el Boletín Oficial, para adaptarse a las obligaciones contenidas en la misma. En dicho plazo, conservarán vigencia el decreto 1172, del 3 de diciembre de 2003, y el decreto 117, del 12 de enero de 2016. Cláusula transitoria 2. Hasta tanto los sujetos pasivos enumerados en el artículo 7° de la presente creen los organismos previstos en el artículo 28, la Agencia de Acceso a la Información Pública creada por el artículo 19 cumplirá esas funciones respecto de los que carezcan de ese organismo.
5	**Decreto 206/2017 Aprueba reglamentación. Ley Nº 27.275.**	Marzo de 2017	Reglamentación artículo 8, incisos varios	a) El carácter reservado, confidencial o secreto de la información clasificada por razones de defensa, política exterior o seguridad interior debe ser dispuesto por normas que reglamenten el ejercicio de la actividad y por acto fundado de las respectivas autoridades competentes, de forma previa a la solicitud de información. En caso de no existir previsión en contrario, la información clasificada como reservada, confidencial o secreta mantendrá ese estado durante DIEZ (10) años desde su producción, transcurridos los cuales, el sujeto obligado deberá formular un nuevo análisis respecto de la viabilidad de desclasificar la información a fin de que alcance estado público. b) Se encuentra específicamente protegido el secreto financiero contemplado en los artículos 39 y 40 de la Ley N° 21.526 y normas concordantes y complementarias y toda aquella normativa que la modifique o reemplace. c) Se entenderá como información cuya revelación pudiera perjudicar el nivel de competitividad o lesionar los intereses del sujeto obligado, aquella que:

Ítem	Norma	Fecha de emisión	Parte / Artículo	Principales Contenidos
				Sea secreta, en el sentido de que no sea, en todo o en las partes que la componen, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y Tenga un valor comercial por ser secreta; y Haya sido objeto de medidas razonables, en las circunstancias, para mantenerla secreta, tomadas por el sujeto obligado que legítimamente la controla. e) La información en poder de la Unidad de Información Financiera exceptuada del acceso a la información pública comprende a toda aquella recibida, obtenida, producida, vinculada o utilizada para el desarrollo de sus actividades en las áreas de seguridad, sumarios, supervisión, análisis y asuntos internacionales y la información recibida de los sujetos obligados enumerados en el artículo 20 de la Ley N° 25.246 y sus modificatorias. i) La excepción será inaplicable cuando el titular del dato haya prestado consentimiento para su divulgación; o cuando de las circunstancias del caso pueda presumirse que la información fue entregada por su titular al sujeto obligado con conocimiento de que la misma estaría sujeta al régimen de publicidad de la gestión estatal; o cuando los datos estén relacionados con las funciones de los funcionarios públicos. Asimismo, los sujetos obligados no podrán invocar esta excepción si el daño causado al interés protegido es menor al interés público de obtener la información. En las causas judiciales donde se investiguen y juzguen casos de graves violaciones a los derechos humanos, genocidio, crímenes de guerra o delitos de lesa humanidad, no serán aplicables las excepciones contenidas en este artículo, debiendo el sujeto obligado suministrar la información requerida en el marco de la causa.
5	**Decreto 206/2017 Aprueba reglamentación. Ley Nº 27.275.**	Marzo de 2017	Reglamentación Artículo 12; Artículo 13; artículo; Artículo 14; Artículo 15	ARTÍCULO 12.- En caso de hacer uso del sistema de tachas, la máxima autoridad del sujeto obligado deberá fundamentar los motivos por los cuales la información no entregada se enmarca en alguna de las excepciones del artículo 8° de la Ley N° 27.275. ARTÍCULO 13.- El acto denegatorio de la solicitud de información deberá ser puesto en conocimiento del solicitante en el lugar de contacto fijado al momento de realizar la solicitud, indicándose las vías de reclamo existentes contra dicho acto, los plazos para su interposición y los requisitos formales establecidos en el artículo 16 de la Ley Nº 27.275. ARTÍCULO 14.- La presentación del reclamo previsto en el artículo 15 de la Ley Nº 27.275 interrumpe el plazo para promover la acción de amparo. ARTÍCULO 15.- El reclamo presentado ante el organismo o entidad requerida deberá ser remitido a la Agencia de Acceso a la Información Pública dentro de los CINCO (5) días hábiles de interpuesto.

Marco normativo: principales resoluciones de AIIP

Ítem	Norma	Nivel y ámbito de aplicación	Fecha Emisión	Principales contenidos
1	**Resolución E 4/2018 AAIP Aprueba criterios orientadores de mejores prácticas de Ley 27.275.** Principalmente dirigidos a la efectividad del reclamo.	Resolución de APN aplica sobre ámbito público	Febrero 2018	Criterio 1. ÁMBITO TEMPORAL para las solicitudes presentadas con anterioridad de la entrada en vigencia de la Ley N° 27.275. Criterio 2. Ante la presentación de un reclamo por incumplimiento de los sujetos obligados, la AAIP solicitará al organismo interviniente, a través de su Responsable de Acceso a la Información Pública, que dentro de los 5 (cinco) días hábiles administrativos desde su notificación, remita toda información que considere necesaria o que obrara en su poder. Criterio 3. La resolución del reclamo por incumplimiento a la Ley N° 27.275 se comunicará a la máxima autoridad del organismo obligado y a su responsable de acceso a la información pública. Criterio 4. INCUMPLIMENTO DE LA OBLIGACIÓN DEL ARTÍCULO 17, INCISO B), SEGUNDO PÁRRAFO. Vencido el plazo de 10 (diez) días hábiles, la AAIP publicará dicho incumplimiento en su página oficial de la red informática. Criterio 5. Cuando el sujeto obligado compruebe que la información requerida no existe o no pueda hallarla debido a razones de fuerza mayor podrá fundar la negativa a proveer la misma demostrando que ha adoptado todas las medidas a su alcance. Criterio 6. COSTOS DE REPRODUCCIÓN. Criterio 7. MEDIOS ELECTRÓNICOS HABILITADOS.
2	**Resolución E 5/2018 AAIP Dirección Nacional de Datos Personales - Obligatoriedad de la intervención**	Resolución de APN aplica sobre ámbito público	Febrero 2018	**Establece como procedimiento interno de la AAIP, la obligatoriedad de la intervención de la D. Nacional de Datos Personales, dependiente de la misma, en los reclamos por incumplimiento previstos en la ley n° 27.275 de acceso a la información pública, que afecten o potencialmente puedan afectar la protección de datos personales, con la finalidad de que esa Dirección emita un informe respecto al caso particular, el que será incorporado al expediente electrónico generado.** **También lo establece en las actuaciones vinculadas a la Ley N° 25.326 de**

Ítem	Norma	Nivel y ámbito de aplicación	Fecha Emisión	Principales contenidos
				Protección de Datos Personales, cuando las mismas pudiesen constituir solicitudes de información pública, con la finalidad de que esa Dirección emita un informe respecto al caso particular, el que será incorporado al Expediente Electrónico generado. En caso de controversia total o parcial entre los informes producidos como consecuencia de las intervenciones referidas en los artículos precedentes, el Director de la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA deberá resolver de manera fundada, debiendo especificar las razones que motivaron la adopción o apartamiento de los informes previamente producidos por las Direcciones Nacionales de cada temática.
3	**Resolución 40/2018 AAIP Aprueba Política Modelo de Protección de Datos Personales para Organismos Públicos**	Resolución de APN – aplica sobre ámbito público	Julio de 2018	**La Resolución aprueba la Política Modelo y recomienda** a los organismos públicos titulares de bases de datos personales **la adopción de la misma o similar,** así como su difusión hacia la ciudadanía. **Asimismo recomienda la designación de un agente de planta permanente como "delegado de protección de datos personales" a quien se le asignará la implementación y el control de cumplimiento interno de la política adoptada.** A través de su ANEXO establece las declaraciones respecto de las pautas que cada organismo adopte para el tratamiento de datos personales y que conforman la política, a saber: • Identificación del tratamiento dado a datos personales por el organismo • Declaración respecto de la inscripción de las bases de datos personales conforme lo estipula la Ley 25.326. • Calidad y finalidad de los datos tratados. • **Pautas de caducidad, confidencialidad y seguridad tomadas para el resguardo de los datos personales tratados que eviten su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones y riesgos.** En caso de detectarse un incidente de seguridad que implique un riesgo significativo para el titular del dato, se comunicará sin dilación tal evento a la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES DE LA AAIP. • Políticas acerca de la cesión de datos personales a entidades públicas o privadas, transferencia internacional, ejercicio de los derechos de acceso, rectificación, supresión, y confidencialidad de los titulares de los datos. • **Declaración de manejo de datos sensibles y en caso afirmativo,**

Ítem	Norma	Nivel y ámbito de aplicación	Fecha Emisión	Principales contenidos
				fundamentación y políticas al respecto. • Declaración de si se contratan tratamientos de datos prestados por terceros.
4	**Resolución 47/2018 AAIP Aprueba Medidas de Seguridad Recomendadas para el Tratamiento y Conservación de Datos Personales en Medios Informatizados como Anexo I. Deroga Disposiciones de la DNPDP N° 11de 2006 y N° 09 de 2008.**	Resolución de APN – aplica sobre ámbito privado	Julio de 2018	La Disposición N° 11 / 2006 establecía medidas de seguridad para el tratamiento y conservación de los datos personales contenidos en bases de datos públicas no estatales y privadas, mientras que la Disposición N° 9 / 2008 establecía los lineamientos indispensables mínimos para el cumplimiento de las normas dictadas en la materia. Ambas son derogadas por la presente en virtud de la evolución vertiginosa de la tecnología e internet, como así también las redes sociales, los servicios de mensajería instantánea y el comercio a través de la red. A fin de adecuarse a las nuevas tecnologías, el ANEXO I establece de modo referencial y con el objetivo de facilitar el cumplimiento de la Ley N° 25.326, las medidas de seguridad recomendadas para la administración, planificación, control y mejora continua de la seguridad de la información, para cada uno de los procesos, tareas y especialidades que las entidades pueden poseer: Recolección de datos, control de acceso, control de cambios, gestión de vulnerabilidades.
5	**Resolución 48/2018 AAIP – Aprueba los criterios orientadores de mejores prácticas en la Ley 27.275.-** Principalmente da pautas para la determinación y el entendimiento del INTERÉS PÚBLICO, con la finalidad de elucidar controversias entre el interés público y la vigencia de otros derechos, así como facilitar el trámite de acceso a la información.	Resolución de APN – aplica sobre ámbito público.	Julio de 2018	Siendo de observancia obligatoria para los sujetos enumerados en el artículo 7°, incisos a), g), h), i), j), k), l), m), n), o), p) y q) de la Ley. Criterio 1. **DETERMINACIÓN DEL INTERÉS PÚBLICO**. El interés público podrá ser entendido como: 1. Información que resulta relevante y beneficiosa para la sociedad en general (excluyendo el mero beneficio individual), constructiva del bien común. 2. Información que afecte intereses o derechos generales. 3. Información referida al proceso político, a la gestión pública y al diseño de los marcos institucionales que gobiernan a la sociedad. 4. Información sobre asuntos necesarios para ejercer el control político sobre las instituciones, para participar en la toma de decisiones públicas que puedan afectar a la sociedad, o para ejercer los derechos políticos; por ejemplo. 5. Información bajo control del Estado relativa a su gestión.

Ítem	Norma	Nivel y ámbito de aplicación	Fecha Emisión	Principales contenidos
				6. Información atinente a personas que actúan en un ámbito público, como funcionarios públicos o políticos. No obstante esto, se deben respetar las legítimas expectativas de privacidad de las figuras públicas de acuerdo a su función. Criterio 2. DERECHO DE INTERÉS PÚBLICO FRENTE A LA VIGENCIA DE OTROS DERECHOS O NORMATIVAS ESPECÍFICAS. 1. Los funcionarios públicos o políticos son las figuras públicas con menor expectativa de privacidad. El ejercicio de una función pública o aspiración a un cargo político necesariamente expone a un individuo a la atención del público (también después de la muerte). 2. Si bien los empleados públicos tienen mayor expectativa de privacidad en comparación a los funcionarios públicos, la información vinculada a remuneración, funciones y demás cuestiones de desempeño deberá considerarse pública. 3. En los casos en que exista conflicto normativo deberán aplicarse criterios de proporcionalidad y determinar el alcance de la restricción. Criterio 3. RESOLUCIÓN DE RECLAMOS. Criterio 4. REMISIÓN DE SOLICITUDES. Cuando la información solicitada no correspondiera al Sujeto Obligado por el que ingresó la actuación, éste deberá: 1. Remitir al Sujeto Obligado que presume tiene la información, o si lo desconociera, a la Agencia de Acceso a la Información Pública, en los términos y alcances del artículo 10 de la Ley N° 27.275. 2. Notificar al solicitante la fecha de derivación. Criterio 5. SOLICITUDES QUE INVOLUCRAN RESPUESTAS DE MÚLTIPLES ORGANISMOS. Principios de informalidad, máxima premura, facilitación e in dubio pro petitor, en pos de garantizar el acceso a la información. Criterio 6. DUDAS SOBRE LA INFORMACIÓN SOLICITADA. Cuando existieran dudas sobre lo solicitado en un pedido, el RAIP deberá comunicarse con el solicitante a fin de realizar las aclaraciones pertinentes. **Criterio 7. SOLICITUD DE ACCESO A LA INFORMACIÓN PÚBLICA SOBRE DATOS PERSONALES PROPIOS.** **En los casos en los cuales una persona presente una solicitud para obtener información vinculada a sus datos personales en poder de un sujeto**

Ítem	Norma	Nivel y ámbito de aplicación	Fecha Emisión	Principales contenidos
				obligado se deberá informar que dicho trámite se trata de un "derecho de acceso" conforme el artículo 14 de la Ley de Protección de Datos Personales. Si quien realizara la solicitud quisiera continuar con el trámite de acceso a la información pública o ya se hubiese caratulado como tal, deberá tramitarse bajo los estándares y criterios propios de la Ley N° 27.275 en tanto, por esta normativa, solo se debe divulgar información si pudiera ser divulgada a cualquier otra persona que la solicitara. Si se entregara la información con datos personales -a pesar que el solicitante fuera el titular del dato- se deberá contar con su consentimiento expreso para la difusión de ellos y adjuntarse dicho consentimiento al expediente.
6	**Resolución 132 /2018 AAIP. Sobre la inscripción, modificación y baja de bases de datos a través de TAD**	Resolución de APN – aplica sobre ámbito público y privado	Octubre 2018	Establece que la inscripción, modificación y baja de las bases de datos personales de carácter privado, publico estatal y público no estatal, que habrán de cumplimentar los responsables de su tratamiento, ante el Registro Nacional de Bases de Datos de la Dirección Nacional de Protección de Datos Personales, deberán tramitarse exclusivamente a través de la plataforma “tramites a distancia” (TAD) o Sistema de Gestión Documental Electrónica (GDE)
7	**Resolución 4 / 2019 AAIP Criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley Nº 25.326.** Define datos biométricos y determina cuándo se considerarán datos sensibles. Además establece pautas para la acreditación del consentimiento del titular respecto de la guarda.	Resolución de APN – aplica sobre ámbito público y privado	Enero 2019	A través de su ANEXO I • Establece pautas para el ejercicio del derecho de acceso a datos personales recolectados mediante sistemas de video vigilancia, criterios respecto de tratamiento automatizado y de disociación de datos. • Define **datos biométricos como aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única.** • Determina cuándo **se considerarán datos sensibles: únicamente cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su titular** (v.g. datos que revelen origen étnico o información referente a la salud). • Establece pautas para la acreditación del consentimiento del titular de los datos a los responsables de su guarda en bases de datos • Determina cuáles son las condiciones de licitud de la cesión de datos personales entre organismos públicos, las que quedan supeditadas a que el cedente haya obtenido los datos en ejercicio de sus funciones, el

Ítem	Norma	Nivel y ámbito de aplicación	Fecha Emisión	Principales contenidos
				cesionario utilice los datos para una finalidad legítima y estricta de acuerdo a su competencia. • Establece pautas para el tratamiento de datos personales de niñas, niños y adolescentes, en particular en cuanto a la expresión de su consentimiento.
8	**Resolución 86 / 2019 AAIP Aprueba GUÍA sobre tratamiento de datos personales con fines electorales.**	Resolución de APN – aplica sobre ámbito privado	Junio 2019	Dado que la Ley N° 25.326 tiene por objeto "la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes" y que el Convenio 108, a su turno, se aplica a todo aquel que realice tratamiento automatizado de datos; por lo que este régimen legal alcanza a las organizaciones y agrupaciones políticas. Apunta a la necesidad de establecer pautas que ayuden a subrayar los puntos clave que deben ser respetados por los partidos políticos cuando tratan datos personales en el curso de actividades electorales (JEPD [2019], Statement 2/2019). Establece una guía sobre tratamiento de datos personales con fines electorales, destinada principalmente a las agrupaciones, organizaciones políticas, candidatos, think tanks, consultores y todo aquel que trate datos personales con el fin de realizar o contribuir en una campaña electoral. Su objetivo es asegurar la integridad y la protección de los datos personales de los ciudadanos participantes con motivo del proceso eleccionario, sentando una serie de lineamientos básicos para alcanzar ese fin, adecuándose a la normativa vigente.

BIBLIOGRAFÍA

Referencias Bibliográficas

[1] Ley N° 25.326 de Protección de Datos Personales y su Decreto Reglamentario 1558 del 29 de noviembre de 2001. http://www.infoleg.gob.ar/

[2] Ley Nº 27.275 de Derecho de Acceso a la Información Pública y normas reglamentarias y complementarias. http://www.infoleg.gob.ar/

[3] David Sarmiento - TOC: ¡No al almacenamiento de datos biométricos en la nube! - 23 enero 2015 - http://www.chw.net/2015/01/toc-no-al-almacenamiento-de-datos-biometricos-en-la-nube/

[4] Isai Rojas González y Gabriel Sánchez Pérez - 2012 - Leyes de protección de datos personales en el mundo y la protección de datos biométricos parte 2 Para Revista .Seguridad UNAM Nro. 14 "Gestión de Seguridad y Riesgos" de septiembre de 2012 (https://revista.seguridad.unam.mx/numeros/numero-14)

[5] 8° Encuentro Nacional de Seguridad de la Información & Ciberseguridad.19 https://www.forosyconferencias.com.ar/evento/Seguridad_de_la_Informacion (accedido el 25/09/2019)

[6] Cuadro comparativo Ley 25.326 de Protección de Datos Personales y Mensaje 147/2018 Proyecto de Ley de Protección de Datos Personales. https://www.argentina.gob.ar/sites/default/files/comparativo_ley_datos.pdf (consulta realizada el 26/09/2019)

[7] Descarga formato XLSX P.2.1 - Total País. Titulares únicos con al menos una jubilación o pensión contributiva. Casos y haberes medios. https://www.anses.gob.ar/informacion/datos-abiertos-pasivos (Accedido el 05/10/2019)

[8] National Institute of Standards and Technology - NIST Biometric Image Software (NBIS) (Consulta efectuada en octubre 2019) https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis.

[9] National Institute of Standards and Technology - Development of NFIQ 2.0 (Consulta efectuada en octubre 2019) https://www.nist.gov/services-resources/software/development-nfiq-20.

[10] Kenneth R. Moses y autores colaboradores: Peter Higgins, Michael McCabe, Salil Prabhakar y Scott Swann CAPÍTULO 6 SISTEMA AUTOMATIZADO DE IDENTIFICACIÓN DE HUELLAS DACTILARES (AFIS) - https://www.ncjrs.gov/pdffiles1/nij/250979.pdf sitio principal https://www.ncjrs.gov/ National Criminal Justice Reference Service. Libro de referencia de las huellas dactilares.

[11] Sitio principal de Neurotechnology Inc. https://www.neurotechnology.com/about.html Brochure institucional https://download.neurotechnology.com/Neurotechnology_Brochure_2019-09-13.pdf Consulta realizada en noviembre de 2019

[12] Sitio principal de Neurotechnology Inc http://neurotechnology.com.ar/megamatcher-references.html Brochure de MegaMatcher SDK en https://download.neurotechnology.com/MegaMatcher_SDK_Brochure_2019-10-03.pdf Consulta realizada en noviembre de 2019

[13] Sitio oficial de la Unión Europea. Área temática normativa sobre protección de datos https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es Consulta hecha el 16/10/2019

[14] Comisión Europea: Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el establecimiento de un marco para la interoperabilidad entre los sistemas de información de la UE de cooperación policial y judicial, asilo y migración - Bruselas, 13.6.2018 COM(2018) 480 final 2017/0352 (COD)

Bibliografía General

1. Asociación por los Derechos Civiles – Área Digital. Artículo “La identidad que no podemos cambiar”- Abril 2017 - https://adcdigital.org.ar.
2. Asociación por los Derechos Civiles – Área Digital. Artículo “Desafíos de la biometría para la protección de los datos personales”- Abril 2017 - https://adcdigital.org.ar.
3. Decreto N° 746 del 25 de septiembre de 2017 complementario a la Ley N° 25.326.
4. Decreto N°899 del 3 de noviembre de 2017 modificatorio de artículo 29 del Anexo I del Decreto Nº 1558/01.

5. Resolución 4/19 de Agencia de Acceso a la Información Pública: Criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley Nº 25.326 y su Anexo I
6. Sitio web ANSES https://www.anses.gob.ar/tramite/registro-de-mi-huella Consulta efectuada el 23/05/2019
7. RESOLUCIÓN ANSES 648 /2014 y su ANEXO II de condiciones funcionales, técnicas y el procedimiento referido al Sistema de Identificación Biométrica.
8. RESOLUCIÓN ANSES 57 E/2017 Por la que se aprueba ANEXO II DE LA RESOLUCION D.E.N Nº 648/14 – Anexo: IF-2017-02690249-ANSES-DGIEIT#ANSES
9. AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA Resolución 15/2018.
10. Resolución 40/2018 AAIP 04-jul-2018. Aprueba documento "POLITICA MODELO DE PROTECCION DE DATOS PERSONALES PARA ORGANISMOS PUBLICOS", ANEXO I (IF-2018-31883807-APN-AAIP)
11. Resolución 47/2018 AAIP 23-jul-2018 – Aprueba documento "MEDIDAS DE SEGURIDAD RECOMENDADAS PARA EL TRATAMIENTO Y CONSERVACION DE LOS DATOS PERSONALES EN MEDIOS INFORMATIZADOS", ANEXO I (IF-2018-34800234-APN-AAIP).
12. Resolución 48/2018 AAIP 26-jul-2018 Criterios orientadores e indicadores de mejores prácticas en la aplicación de la ley N° 27.275 - ANEXO I (IF-2018-35695088-APN-AAIP)
13. Resolución 132/2018 AAIP 19-oct-2018 – Sobre procedimientos de inscripción, modificación y baja de bases de datos personales.
14. Disposición 12/2010 Dirección Nacional de Protección de Datos Personales 18-jun-2010 Tratamientos de datos personales destinados a difusión pública.
15. AAIP Resolución 132/2018 RESOL-2018-132-APN-AAIP - Inscripción, modificación y baja de las bases de datos personales.
16. Resolución 86/2019 AAIP – Guía sobre tratamiento de datos personales con fines electorales.
17. Publicación digital "Punto a Punto". Artículo del 6 marzo, 2017 https://puntoapunto.com.ar/chau-tarjetas-se-vienen-las-huellas-dactilares-en-los-cajeros-automaticos/
18. Boletín AFIP- Bol. Imp. Nº 258 – Enero 2019 - http://200.1.116.22/pdfp/BOL_DGI_0258_1_2019.PDF

19. COUNCIL OF EUROPE - BIOM F Comité consultivo de la convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal (T-PD) Estrasburgo, febrero de 2005 T-PD (2005) Informe de situación relativo a la aplicación de los principios de la Convención 108 a la recogida y al proceso de los datos biométricos (traducción al español no oficial realizada por la agencia española de protección de datos del documento original en inglés)
20. UNION EUROPEA – DOCUMENTO DE TRABAJO SOBRE BIOMETRÍA - Adoptado el 1 de agosto de 2003 por el Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.(MARKT/12168/02/ES WP 80) - http://www.informatica-juridica.com/documento-trabajo/documento-trabajo-biometria/
21. UNAM - Facultad de Ingeniería Biometría Informática -Clasificación de Sistemas: Reconocimiento de Huellas - http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/recohuella.html
22. Agencia Española de Protección de Datos (AEPD) y Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain - CÓDIGO DE BUENAS PRÁCTICAS EN PROTECCIÓN DE DATOS PARA PROYECTOS BIG DATA Web: http://www.agpd.es y http://www.ismsforum.es
23. GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 Dictamen 05/2014 sobre técnicas de anonimización -2014- (Grupo de Trabajo fue creado en el artículo 29 de la Directiva 95/46/CE. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE)
24. OEA - FORO e-GOBIERNO OEA | BOLETÍN ED 79 “e-Gobierno y Gestion de Identidades” Noviembre 2012
25. National Institute of Standards and Technology ANSI/NIST-ITL 1-2011 Information Technology: American National Standard for Information Systems Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information - http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=910136
26. Jorge Domínguez. Artículo “Biometría Espectral” para Revista Seguridad en América – Año 18 – N°104 Septiembre / Octubre 2017 – México. https://issuu.com/revistaseguridadenamerica/docs/seguridad_en_am__rica_104

27. Luis Eduardo Gómez - Artículo “Protegiendo Información Sensible” para Revista Seguridad en América – Año 17 – N°98 Septiembre / Octubre - 2016 - México https://issuu.com/revistaseguridadenamerica/docs/seguridadenamerica_98
28. Glosario de Términos de Ciberseguridad - Anexo II IF-2019-78455467-APN-SGM#JGM de Resolución 2019-1523-APN-SGM#JGM del 12/09/2019.