Ministerio de Justicia y Derechos Humanos

Dirección Nacional de Protección de Datos Personales

REF: EXP-S04:0056881/2011

DICTAMEN DNPDP N° 16/11

BUENOS AIRES, 4 de octubre de 2011

SEÑOR SUBSECRETARIO:

Se da intervención a esta Dirección –en su carácter de órgano de control y autoridad de aplicación de la Ley 25.326 de Protección de Datos Personales- con relación al proyecto de decreto a través del cual se propicia la creación del PROGRAMA NACIONAL DE ESTANDARIZACIÓN DE DATOS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES (en adelante el Proyecto) dentro del ámbito de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE.

- I -

ANTECEDENTES

El proyecto de creación del PROGRAMA NACIONAL DE ESTANDARIZACIÓN DE DATOS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES en el ámbito de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN, tiene por finalidad crear, adoptar y establecer para el ámbito público nacional los estándares adecuados al empleo de componentes necesarios para la utilización de las herramientas biométricas y biométricas forenses, teniendo presente la necesidad de un empleo eficiente y coordinado de los recursos de las Tecnologías de la Información y las Comunicaciones por parte del Estado Nacional.

Prevé asimismo la creación en dicho ámbito de una BASE DE DATOS DE REGISTROS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES.

Asimismo, y en lo que resulta relevante para la protección de datos personales, el PROGRAMA NACIONAL DE ESTANDARIZACIÓN DE DATOS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES desarrollará las siguientes actividades: Sistematizar y actualizar la Base de Datos de Registros Biométricos y Biométricos Forenses; Establecer el intercambio …con los gobiernos y organismos internacionales vinculados en materia biométrica y biométrica forense; Relevar, elaborar, supervisar y documentar los procedimientos actuales en materia biométrica y biométrica forense…; Propiciar las herramientas biométricas necesarias para su incorporación en el Gobierno Electrónico, Pasaporte Electrónico y Voto Electrónico entre otros, a los fines de brindar mayor seguridad a los procesos; Estudiar e informar los métodos necesarios de seguridad a implementar en los procesos biométricos y biométricos forenses a los fines de garantizar la privacidad de los datos; Difundir y promover el uso de las herramientas biométricas y biométricas forenses.

Prevé, entre sus considerandos, observar la Ley Nº 25.326 en las actividades relativas al tratamiento de la información, otorgando seguridad, como también, en el art. 4 inc. 11 del proyecto, prevé garantizar la privacidad de los datos.

Con anterioridad a la presente consulta han emitido opinión favorable la OFICINA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN, la OFICINA NACIONAL DE INNOVACIÓN DE GESTIÓN, la SECRETARÍA LEGAL Y TÉCNICA de Presidencia de la Nación a fs. 30/34, y la DIRECCIÓN DE ASESORÍA TÉCNICA de la SECRETARÍA LEGAL Y TÉCNICA a fs. 36, recomendando, estos dos últimos, la intervención de esta Dirección Nacional de Protección de Datos Personales.

En este estado se encuentran las presentes actuaciones para emitir opinión.

- II -

ANÁLISIS

En lo que resulta de interés para el presente análisis, el PROGRAMA NACIONAL DE ESTANDARIZACIÓN DE DATOS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES prevé: a) La creación de una BASE DE DATOS DE REGISTROS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES; y b) el desarrollo de estándares biométricos en el ámbito del Estado Nacional (Ley Nº 24.156) (en particular en cuestiones como el Gobierno Electrónico, Pasaporte Electrónico y Voto Electrónico), procedimientos, seguridad y privacidad.

En cuanto a la protección de datos personales, cabe analizar las acciones previstas según las disposiciones de la Ley Nº 25.326: a) Requisitos para la creación de un nuevo banco de datos; y b) Requisitos de licitud del tratamiento de datos previsto.

a) Requisitos de creación de la BASE DE DATOS DE REGISTROS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES (art. 22 de la Ley Nº 25.326):

Para la implementación de la BASE DE DATOS DE REGISTROS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES resulta necesario una disposición general publicada en el Boletín Oficial de la Nación o diario oficial, requisito que se vería cumplido con la publicación del decreto previsto en el Boletín Oficial.

Ahora bien, toda norma de implementación de una base de datos debe cumplir con los requisitos establecidos en el inciso 2° del artículo 22 de la Ley N° 25.326: a) Características y finalidad del archivo; b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas; c) Procedimiento de obtención y actualización de los datos; d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán; e) Las cesiones, transferencias o interconexiones previstas; f) Órganos responsables del archivo, precisando dependencia jerárquica en su caso; g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

Al respecto, al momento de considerarse la finalidad de la BASE DE DATOS DE REGISTROS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES y el tratamiento de datos personales previsto, debe tenerse presente uno de los principio generales de la protección de datos personales: limitar al mínimo indispensable el tratamiento de los datos, de manera tal que no implique un mayor riesgo para su titular.

b) Requisitos de licitud del tratamiento de datos personales previsto:

El desarrollo de estándares biométricos en el ámbito del Estado Nacional, sus procedimientos, seguridad y privacidad, requiere considerar las disposiciones de la Ley Nº 25.326.

En tal sentido, se recomienda tener en cuenta las disposiciones de la Ley Nº 25.326 en caso de realizar tratamientos de datos personales en las siguientes actividades previstas por el proyecto: i) sistematizar y actualizar la Base de Datos de Registros Biométricos y Biométricos Forenses; ii) Establecer el intercambio …con los gobiernos y organismos internacionales vinculados en materia biométrica y biométrica forense; iii) Relevar, elaborar, supervisar y documentar los procedimientos actuales en materia biométrica y biométrica forense…; iv) Propiciar las herramientas biométricas necesarias para su incorporación en el Gobierno Electrónico, Pasaporte Electrónico y Voto Electrónico entre otros, a los fines de brindar mayor seguridad a los procesos; v) Estudiar e informar los métodos necesarios de seguridad a implementar en los procesos biométricos y biométricos forenses a los fines de garantizar la privacidad de los datos; vi) Difundir y promover el uso de las herramientas biométricas y biométricas forenses.

El proyecto bajo análisis requiere una particular consideración de los siguientes requisitos de licitud del tratamiento de datos personales: 1) el cumplimiento del requisito de calidad del dato en el tratamiento previsto; 2) la eventual cesión de los datos a terceros; y 3) la obligación de inscripción.

1) Calidad del dato:

Determinar el cumplimiento de los requisitos de calidad del dato de la Ley Nº 25.326, requiere analizar dos aspectos: 1) Categoría de los datos a tratar (nos permitirá verificar si los datos son de tratamiento permitido o prohibido, como también los requisitos específicos a que puedan ser sometidos en razón de su calidad); y 2) Tratamiento al que serán sometidos (nos permite analizar su pertinencia y demás requisitos de calidad de los datos objeto de tratamiento; como también los requisitos para su recolección y cesión a terceros).

1.1. Categoría de los datos a tratar[1]

Conforme cabe deducirse de la descripción del proyecto arriba efectuada, la naturaleza de los datos objeto de tratamiento serían básicamente datos identificatorios y biométricos.

Los datos meramente identificatorios (art. 5º inc. 2 punto "c" de la Ley Nº 25.3.26) son una categoría que no requiere particulares consideraciones, y se les aplica las generalidades de la ley.

Los datos biométricos son una categoría específica de los datos identificatorios, que resultan de la conversión de aspectos físicos o conductuales de la persona en datos que tienen por finalidad identificar a su titular. Podemos distinguir los siguientes métodos biométricos más usados: firma, huella dactilar, ADN, facial, ocular, palmar, voz.

Caben ser calificados entre los datos identificatorios pues si bien la biometría se sustenta en aspectos concretos de la persona alcanzados por el derecho a la privacidad (iris, la

[1] Ver al respecto TRAVIESO, Juan Antonio, "La protección de los datos personales y la Biometría", BIOMETRIAS, publicación de la Jefatura de Gabinete de Ministros con motivo del V Congreso Internacional de Biometría en la República Argentina, Noviembre de 2010.

huella dactilar, etc.), el dato objeto de tratamiento en la actividad biométrica no es propiamente el iris de la persona, sino el “algoritmo” que deriva del mismo, o sea, la métrica derivada de dicho hecho concreto.

En tal sentido, la privacidad de las personas tiene particular incidencia al momento de la recolección del dato biométrico, o sea, cuando la tecnología se acerque al cuerpo de la persona y obtenga sus características personales, luego, el dato en principio ya no será íntimo, sino identificatorio.

Cabe distinguir en este punto la existencia de datos íntimos de la persona (núcleo inaccesible y prohibido) de aquellos datos alcanzados por la esfera de la privacidad en diversos grados de protección.

En tal sentido, cabe considerar que fuera del núcleo de lo íntimo, bastará con una autorización legal, derecho o interés legítimo para no configurar una intromisión arbitraria en la privacidad de las personas. Circunstancias cuya determinación dependerá del caso concreto.

Los datos biométricos que esta Dirección Nacional entiende que pueden motivar el presente análisis (firma, huella dactilar, ADN, facial, ocular, palmar, voz) en cuanto representan una manifestación externa de la persona caben ser considerados dentro del género de datos alcanzados por esferas de la privacidad externas al núcleo íntimo.

En tal sentido, al momento de la formación del dato biométrico, al ser parte de la privacidad de la persona, sería exigible el consentimiento previo del titular del dato previo a su recolección, salvo que exista un interés legítimo suficiente, derecho o autorización legal que permita acceder a dicha información, de forma tal que no se produzca una intromisión arbitraria en la intimidad de las personas (art. 1071 bis. Cod. Civil) y siempre se respete su dignidad.

A modo de ejemplo podemos citar la utilización de la fotografía, la huella digital, y, excepcionalmente, del iris, en el ámbito laboral. Al respecto, las normativas del trabajo otorgan al empleador facultades organizativas (Capítulo VII de la ley 20.744), en la medida que se resguarde la dignidad del trabajador y sus datos personales, entre las cuales cabe considerar incluida la utilización de datos biométricos en caso que medien razones fundadas.

Esta actividad tecnológica requiere tomar ciertos recaudos para no dañar a terceros con motivo de su funcionamiento. El principal recaudo será resguardar a los datos biométricos objeto de tratamiento con las medidas de seguridad necesarias para evitar accesos indebidos a los bancos de datos o sustracciones de dichos datos.

Asimismo, debe evitarse un uso inadecuado de la biometría, como sería otorgarle un valor indubitable a toda prueba biométrica y/o tomar decisiones que requieren juzgar conductas humanas basadas exclusivamente en datos biométricos, dado que no es un medio infalible.

Ahora bien, a través del principio de calidad del dato se pretende que todo tratamiento de datos personales reúna una serie de cualidades que definan al dato como ajustado a derecho, siempre en relación a la finalidad del tratamiento.

El análisis de la calidad del dato requiere tanto un análisis intrínseco de la información como también en relación con las distintas variables del tratamiento, teniendo en cuenta que siempre incluye el aspecto dinámico o referencial, o sea, en relación con la finalidad del tratamiento al cual se lo va a destinar.

En nuestro ordenamiento positivo, los principios axiológicos se determinan en el art. 4º de la ley 25.326, que requiere verificar, en relación al ámbito y finalidad del tratamiento, que los datos sean: 1) adecuados; 2) pertinentes; 3) no excesivos; 4) ciertos; 5) exactos, de ser necesario; 6) actualizados, de ser necesario; 7) completos; 8) caducidad del dato.

En tal sentido, cabe tener presente el alcance de los mismos para su correcta aplicación al caso bajo análisis, conforme pasa a desarrollarse.

El principio de dato **adecuado** requiere analizar el ajuste o proporcionalidad del dato con su tratamiento, aplicando un criterio de razonabilidad. La amplitud y riqueza del concepto de este principio lo convierte en una de las claves de la calidad del dato.

La **pertinencia** del dato tiene estrecha vinculación con los conceptos de necesidad, relevancia, oportunidad, conveniencia e interés, frente a la finalidad del tratamiento. En tal sentido, el dato será pertinente cuando sea realmente necesario, relevante, oportuno, conveniente y de interés para la finalidad del tratamiento. El dato que no es relevante para la finalidad, deja de ser pertinente.

En cuanto a la **no excesividad** del dato se debe evaluar mediante un juicio de razonabilidad, limitando el uso y tratamiento de la información personal a la estrictamente necesaria para la finalidad pretendida; y es aplicable tanto al momento de la recolección como durante todo el tratamiento de los datos. Este principio es particularmente aplicable a la presente actividad al poner en juego la privacidad del titular del dato.

El requisito de **certeza** exige que la información se condiga lo máximo posible con la realidad sobre la que se pretende informar. Esta adecuación debe operar de manera tal que se produzca un razonable espejo informativo, e incluye dentro de sí el concepto de veracidad.

Los datos deben ser **exactos y actualizados** en caso que fuere necesario. El nivel de exactitud y actualización dependerá de la finalidad del banco de datos, por lo que se deberá analizar cada caso concreto. Dadas las características del Proyecto, la exactitud de los datos es un requisito sustancial para su correcto funcionamiento.

Deberán disponerse las medidas que garanticen dicha exactitud y de ser necesario su actualización permanente, como así también las medidas necesarias para proceder a su corrección en caso de error.

La **completitud** es un principio que nuestra ley diseña como de carácter pasivo, o sea, se completará el dato cuando el responsable “tenga conocimiento” de que los datos en su poder son incompletos, o sea, no siempre el responsable del archivo estará obligado a completarlos. Ahora bien, hay casos en los cuales las características del tratamiento exigen del responsable del banco de datos tomar los recaudos necesarios para que los datos sean siempre completos.

Otro principio de calidad del dato es el de **caducidad**, que prevé el caso en el cual los datos, con posterioridad a su recolección y por el mero transcurso del tiempo, pierden su calidad inicial de datos pertinentes y en consecuencia deben ser destruidos.

Al respecto del análisis de calidad del dato biométrico, esta Dirección Nacional ya ha

emitido opinión en los DICTÁMENES DNPDP Nros. 242/05, 01/09, 02/09 y 15/09, 14/10, manteniendo el criterio allí expuesto para el presente caso.

En dichos dictámenes se ha señalado como lícito el tratamiento de datos biométricos, siempre y cuando resulten estrictamente necesarios para la finalidad pretendida, verificando la no afectación de la intimidad de las personas (artículo 4º de la Ley Nº 25.326).

En tal sentido, previo a todo tratamiento de datos biométricos debe evaluarse si la recolección de los datos se presenta como una medida estrictamente necesaria para la finalidad pretendida, y no exista otra más razonable (menos invasiva de la privacidad); y que la finalidad y circunstancias que la motivan son proporcionadas a la calidad del dato a utilizar.

En los mismos se señaló la adecuación del dato biométrico, como ser el caso de la utilización de huellas dactilares, que tiene referencia a la privacidad por ser una característica física de las personas -amparada por nuestro derecho, tanto por el art. 1071 bis del Código Civil como por Tratados Internacionales de rango constitucional-, pero que dado el carácter básicamente identificatorio de los datos biométricos se admite su tratamiento por terceros bajo ciertas situaciones y condiciones.

Se citó también, en el plano internacional, la 27º Conferencia Internacional de Comisionados de Protección de Datos y Privacidad celebrada en la Ciudad de Montreux, Suiza, donde por propuesta del Comisionado Federal de Protección de Datos de Alemania y con el apoyo de la Dirección Nacional de Protección de Datos Personales de la República Argentina, de la Comisión de Protección de Datos de Austria y la Comisión de Protección de Datos de Italia, se aprobó el día 16 de septiembre de 2005 la "Resolución sobre el uso de información biométrica en pasaportes, identificaciones y documentos de viaje", donde se advierte del peligro inherente al tratamiento de datos biométricos llamando a: 1) implementar urgentes medidas para limitar el riesgo de la biometría; 2) distinguir la recolección de datos para fines públicos por obligación legal, de la realizada por el sector privado en base al consentimiento del titular del dato; 3) el establecimiento de restricciones técnicas para limitar el uso de la biometría para verificar la identidad en pasaportes cuando el titular presente su documento[2].

En igual ámbito internacional cabe resaltar el Documento de Trabajo sobre biometría de fecha 1 agosto de 2003 del Grupo de trabajo del artículo 29 de la Directiva 95/46/CE, del que cabe destacar: a) Principio de fines y proporcionalidad: El cumplimiento de este principio implica en primer lugar una determinación clara de los fines para los que se recogen y tratan los datos biométricos. Por otra parte, hace falta evaluar el cumplimiento de la proporcionalidad y de la legitimidad, teniendo en cuenta los riesgos para la protección de los derechos y libertades fundamentales de las personas y especialmente si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva. La proporcionalidad ha sido el criterio principal en casi todas las decisiones adoptadas hasta ahora por las autoridades encargadas de la protección de datos sobre el tratamiento de datos biométricos. Para fines de control de acceso (autenticación/comprobación), el Grupo opina que los sistemas biométricos relativos a características físicas que no dejan rastro (por ejemplo la forma de la mano, pero no las huellas

---

[2] En ingles, el texto literalmente dice: "The Conference calls for: 1. effective safeguards to be implemented at an early stage to limit the risks inherent to the nature of biometrics, 2. the strict distinction between biometric data collected and stored for public purposes (e.g. border control) on the basis of legal obligations and for contractual purposes on the basis of consent, 3. the technical restriction of the use of biometrics in passports and identity cards to verification purposes comparing the data in the document with the data provided by the holder when presenting the document".

digitales) o los sistemas biométricos relativos a características físicas que dejan rastro pero no dependen de la memorización de los datos poseídos por una persona distinta del interesado (en otras palabras, los datos no se memorizan en el dispositivo de control de acceso ni en una base de datos central) crean menos riesgos para la protección de los derechos y libertades fundamentales de las personas. Diversas Autoridades encargadas de la protección de datos han respaldado esta opinión y han declarado que sería preferible no almacenar la biometría en una base de datos sino más bien sólo en un objeto disponible exclusivamente para el usuario, como una tarjeta con microchip, un teléfono móvil o una tarjeta bancaria. Dicho de otro modo, las aplicaciones de autenticación/comprobación que se pueden llevar a cabo sin un almacenamiento centralizado de datos biométricos no debería suponer la utilización de excesivas técnicas de identificación; b) Obtención leal e información sobre el interesado: El tratamiento de datos biométricos y en particular su recogida se realizará de manera leal. El responsable del tratamiento informará al interesado de conformidad con los artículos 10 y 11 de la Directiva 95/46/CE, lo cual incluye concretamente la definición exacta de los fines y la identidad del responsable del tratamiento del registro (que será frecuentemente la persona encargada del sistema biométrico o de la técnica biométrica). Deben evitarse los sistemas que recogen datos biométricos sin el conocimiento de los interesados. Algunos sistemas biométricos como el reconocimiento facial a distancia, la recogida de huellas digitales o la grabación de la voz presentan más riesgos desde este punto de vista; c) Datos sensibles: Determinados datos biométricos podrán considerarse sensibles en el sentido del artículo 8 de la Directiva 95/46/CE y, en particular, los datos que revelen el origen racial o étnico o los datos relativos a la salud. Por ejemplo, en sistemas biométricos basados en el reconocimiento facial, se pueden tratar los datos que revelan el origen racial o étnico. En esos casos, se aplicarán las garantías especiales contempladas en el artículo 8 además de los principios generales de protección de la Directiva. Esto no significa que todo tratamiento de datos biométricos vaya a incluir necesariamente datos sensibles. Si un tratamiento contiene datos sensibles es una cuestión de apreciación vinculada con la característica biométrica específica utilizada y la aplicación biométrica en sí. Es más probable que eso ocurra en caso de tratamiento de datos biométricos en forma de imágenes, porque en principio los datos brutos no se pueden reconstruir a partir de la plantilla".

De lo hasta aquí expuesto, esta Dirección Nacional concluye respecto de la calidad de los datos biométricos que los mismos requerirán particular atención por la potencialidad que poseen de afectar los derechos de sus titulares, debiendo analizarse en cada caso concreto de tratamiento si su utilización cumple con el deber de proporcionalidad y pertinencia, o sea, si el tratamiento de dichos datos es adecuado a la finalidad prevista y si no resultan una desproporcionada y/o arbitraria intromisión en la intimidad de los titulares de dichos datos.

No sería arbitrario, por ejemplo: Requerir las huellas digitales si para la actividad prevista es necesario tener una alta certeza sobre la identidad de la persona; Si se requiere la firma y la misma es necesaria para verificar la real presencia de la persona en dicho acto.

1.2. Restantes principios:

Asimismo, se deben verificar y ejecutar las medidas necesarias para el adecuado cumplimiento de los restantes principios y requisitos de licitud del tratamiento de datos establecidos por la Ley Nº 25.326 en su Capítulo II, como ser, en particular: a) Requisitos de

licitud de los bancos de datos (art. 3º, 21 y 22 de la Ley Nº 25.326); b) Adecuada recolección de los datos (art. 5º y 6º Ley Nº 25.326); c) Prever mecanismos para que el titular del dato posea información sobre el tratamiento de su información personal (art. 6º Ley 25.326); d) En caso de ser pertinente, prever el consentimiento del titular del dato; e) Desarrollar procedimientos para cumplir con los derechos del titular del dato (acceso, rectificación y supresión) (art. 14, 15 y 16 Ley Nº 25.326); f) Seguridad y confidencialidad del Banco de Datos (art. 9º y 10 Ley Nº 25.326); g) No automaticidad (art. 20 de la Ley Nº 25.326).

a) Requisitos de licitud de los bancos de datos (art. 3º, 21 y 22 de la Ley Nº 25.326)

La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos en el Registro Nacional de Bases de Datos de la DNPDP, observando en su operación los principios que establece la Ley Nº 25.326.

En particular, debe verificarse el cumplimiento de los requisitos del art. 22 para la creación de bancos de datos públicos, que se analiza en punto separado.

b) Recolección de datos en la forma prescripta por la ley 25.326.

La recolección de datos personales por parte de Organismos Públicos, como resulta en el presente caso, no requiere del consentimiento del titular del dato si son recolectados en virtud de una disposición legal o en ejercicio de funciones propias de los poderes del Estado (art. 5 inc. 2, punto b, de la Ley Nº 25.326).

Debe entonces verificarse si al momento de recolectarse los datos biométricos se realiza en cumplimiento de la competencia del organismo u obligación legal.

c) Información al titular del dato:

En cuanto al requisito de información que prevé la Ley Nº 25.326, el Proyecto debería incluir los requisitos del art. 6º de la Ley Nº 25.326: “ARTICULO 6° — (Información). Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos”.

Se debe tener presente dicho requisito al momento de recolectar la información biométrica y durante el funcionamiento de la Base de Datos a crear.

d) Consentimiento del titular del dato;

Conforme a lo ya expuesto, en la medida que los datos sean tratados en cumplimiento de una disposición legal o en ejercicio de las funciones asignadas por ley al organismo, no será necesario el consentimiento del titular del dato.

e) Derechos del titular del dato de acceso, rectificación y supresión (art. 14, 15 y 16 Ley Nº 25.326)

La Ley Nº 25.326 regula en su artículo 14 el derecho del titular del dato a acceder a la información registrada y en el artículo 16 la facultad de rectificarla y actualizarla.

Al momento de implementar la BASE DE DATOS DE REGISTROS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES deberá prever la entrega de la información personal que soliciten los titulares y permitirles su rectificación y/o su supresión (art. 14, 15, 16 y 17 de la Ley Nº 25.326), salvo que por ley se disponga lo contrario y/o en los casos de excepción previstos por los arts. 16 y 17 de la Ley Nº 25.326[3].

f) Seguridad y confidencialidad del Banco de Datos

La BASE DE DATOS DE REGISTROS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES debe reunir condiciones de seguridad y confidencialidad de la información personal almacenada conforme a lo requerido por los artículos 9º y 10 de la Ley 25.326[4].

g) No automaticidad (art. 20 de la Ley Nº 25.326)

Ya se ha señalado la necesidad de evitar un uso inadecuado de la biometría, como sería tomar decisiones que impliquen evaluar conductas de las personas basadas exclusivamente en el procesamiento de datos biométricos, dado que solo son herramientas auxiliares del juicio y eventualmente falibles.

El art. 20 de la Ley Nº 25.326 expresamente dispone que “las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado”, tachando de nulidad a dichos actos.

---

[3] **ARTICULO 17.** — (Excepciones). 1. 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. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado. 3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

[4] **ARTICULO 9°** — (Seguridad de los datos). 1. 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, 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. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad. **ARTICULO 10.** — (Deber de confidencialidad). 1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

2) Cesiones:

Respecto a eventuales cesiones de datos desde o hacia la BASE DE DATOS DE REGISTROS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES, deberá verificarse, además del cumplimiento de la normativa específicamente aplicable, el cumplimiento del art. 11 de la Ley Nº 25.326, particularmente que la cesión entre Organismos sea directa y que la categoría del dato a ceder no exceda la competencia del cesionario, o sea, que la competencia lo habilite para recibir dicha información sin que sea un dato excesivo o inadecuado para sus funciones (categoría y calidad del dato adecuada).

3) Obligación de inscripción:

En cuanto a la consulta sobre la necesidad de inscribir dicho banco de datos, cabe recordar que el artículo 3º y 21 de la Ley Nº 25.326 establecen la obligatoriedad de la inscripción en el Registro de Bases de Datos como requisito de licitud, por lo que se deberá a proceder a su inscripción previo a su funcionamiento.

-III-

Conclusión

Conforme con lo expuesto y en lo que hace a la competencia específica de esta Dirección Nacional de Protección de Datos Personales, se concluye respecto de la presente consulta:

1) En la medida que se de cumplimiento a lo recomendado y se verifique la adecuación del proyecto a los principios expuestos, **no se detecta óbice para la medida bajo análisis.**

2) La creación de la BASE DE DATOS DE REGISTROS BIOMÉTRICOS Y BIOMÉTRICOS FORENSES debe **cumplir con el requisito dispuesto en el art. 22 de la Ley Nº 25.326.**

3) Oportunamente, deberá procederse a la **inscripción de la Base de Datos** prevista en el Registro Nacional de Bases de Datos a cargo de esta Dirección Nacional.

Saluda a usted muy atentamente.

Dr. Juan Antonio TRAVIESO
DIRECTOR NACIONAL DE PROTECCIÓN
DE DATOS PERSONALES

AL SR. SUBSECRETARIO DE TECNOLOGÍAS DE GESTIÓN
DE LA SECRETARIA DE LA GESTIÓN PÚBLICA
DE LA JEFATURA DE GABINETE DE MINISTROS
EDUARDO A. THILL
S / D