THĒMIS-Revista de Derecho 67. 2015. pp. 131-140. ISSN: 1810-9934

EL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES. ALGUNOS TEMAS RELEVANTES DE SU REGULACIÓN EN EL PERÚ

THE RIGHT TO PERSONAL DATA PROTECTION. SOME RELEVANT TOPICS ABOUT ITS REGULATION IN PERU

Francisco José Eguiguren Praeli*
Pontificia Universidad Católica del Perú
Miembro del Consejo Consultivo de THĒMIS

What guarantees do we have as titleholders of the right to personal data protection? Does the Political Constitution of 1993 truly protect this right in a properly way? Which role does the relatively recent Peruvian Law on the Personal Data Protection play to that effect?

In this article, the renowned constitutionalist gives answers to these questions with a brief and detailed analysis of the Peruvian Law on the Personal Data Protection and its rules of procedure, focusing in its pros and cons, but also of the Peruvian National Personal Data Protection Authority's role and functions to that effect.

Key Words: Habeas data; right to informational self-determination; Peruvian Law on the Personal Data Protection; Peruvian National Personal Data Protection Authority.

¿Qué garantías tenemos como titulares del derecho a la protección de datos personales? ¿Realmente la Constitución Política de 1993 tutela adecuadamente este derecho? ¿Qué rol juega al respecto la relativamente reciente Ley de Protección de Datos Personales?

En el presente artículo, el reconocido constitucionalista da respuesta a estas cuestiones con un breve pero detallado análisis de la Ley de Protección de Datos Personales y su reglamento, incidiendo en sus ventajas y desventajas, así como del rol y funciones de la Autoridad Nacional de Protección de Datos Personales al respecto.

Palabras clave: Hábeas data; autodeterminación informativa; Ley de Protección de Datos Personales; Autoridad Nacional de Protección de Datos Personales.

* Abogado. Doctor en Humanidades y Magíster en Derecho Constitucional por la Pontificia Universidad Católica del Perú (PUCP). Ex Ministro de Justicia y Derechos Humanos. Ex embajador del Perú en el Reino de España y en el Principado de Andorra. Ex Juez ad hoc en la Corte Interamericana de Derechos Humanos. Ex Presidente de la Asociación Peruana de Derecho Constitucional. Ex Director Ejecutivo de la Comisión Andina de Juristas. Ex Director General de la Academia de la Magistratura. Ex Jefe del Departamento Académico de Derecho de la PUCP. Ex Miembro del Consejo Directivo de la Asociación Civil Transparencia. Ex consultor de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, del Instituto Interamericano de Derechos Humanos, de la Agencia de los Estados Unidos para el Desarrollo, de la Organización Internacional para las Migraciones, entre otros. Profesor en la Facultad de Derecho y en la Escuela de Postgrado de la PUCP. Director de la Maestría en Derecho Constitucional de la PUCP. Miembro electo de la Comisión Interamericana de Derechos Humanos. Contacto: feguigu@pucp.edu.pe.

Nota del editor: El presente artículo fue recibido por el Consejo Editorial el día 03 de junio de 2015, y aceptado por el mismo el 02 de julio de 2015.

I. INTRODUCCIÓN

Una de las escasas novedades positivas que introdujo la Constitución de 1993 en materia de derechos fundamentales, ya que su orientación general en este campo fue más bien regresiva, fue el reconocimiento del derecho de toda persona a ejercer control sobre el registro, tratamiento y difusión de sus datos personales. Así, en el numeral 6 del artículo 2 de nuestra Carta Política, se establece que "[…] los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar".

Tuvieron que pasar bastantes años antes de que se dictaran las normas específicas destinadas al desarrollo y regulación de este derecho constitucional. Cabe así mencionar la Ley 29733, Ley de Protección de Datos Personales [en adelante, LPDP] –publicada el 3 de julio de 2011–, y el reglamento de la misma, aprobado por Decreto Supremo 003-2013-JUS [en adelante, el reglamento] y publicado el 22 de marzo de 2013.

En el presente trabajo, analizaremos algunos de los aspectos más relevantes contenidos en la LPDP y su reglamento, en especial de aquellos que pueden tener mayor incidencia respecto a lo estipulado en el precepto constitucional, con el fin de apreciar los aportes y limitaciones que pueden conllevar para la mejor protección y el ejercicio de este derecho fundamental.

II. DE LAS CARENCIAS DEL PRECEPTO CONSTITUCIONAL AL INTENTO POR SUPERARLAS EN EL CÓDIGO PROCESAL CONSTITUCIONAL

El derecho a la protección de los datos personales es conocido en la doctrina constitucional como "autodeterminación informativa" o "libertad informática". A partir de su reconocimiento constitucional en la jurisprudencia, especialmente en Alemania, se dice que este derecho está referido a la facultad del titular de los datos personales a determinar quién, qué, cuándo y con qué motivo puede conocer los datos que a aquél están referidos.

Sin perjuicio de resaltar la importancia del reconocimiento de este derecho en la vigente Constitución peruana, cabe advertir que –lamentablemente– el texto del precepto resulta muy insuficiente, en cuanto a su contenido, y deficiente, en cuanto a su redacción, lo que determina que adolezca de muchas carencias –desde el punto de vista conceptual y técnico– respecto a los alcances y protección de este derecho. Así, por ejemplo:

a) La referencia que hace la norma a los "servicios informáticos" resulta muy imprecisa, tanto sobre el tipo de institución u organización incursa en esta disposición constitucional como sobre la actividad involucrada. Y es que la expresión "servicios informáticos", con relación al tratamiento de los datos personales, podría dar a entender que la protección de este derecho se extiende exclusivamente a las entidades públicas o privadas que proporcionan este tipo de información a terceros ("servicios"), pudiendo quedar excluidos los registros o bancos de datos existentes que no brindan servicio ni acceso al público.

b) La norma constitucional sólo protege expresamente la posibilidad de que el titular de los datos personales pueda impedir que éstos sean suministrados a terceros; omitiendo así componentes esenciales de este derecho, reconocidos en otras normas constitucionales o legales comparadas, como el poder acceder a la información personal contenida en los registros o bases de datos, conocer su contenido, tener la facultad de corregirla o actualizarla (de ser inexacta), o de hacer suprimir la información personal indebidamente registrada.

c) El único motivo que se menciona como fundamento para que el titular del derecho pueda demandar que no se suministren sus datos personales a terceros, es para proteger su intimidad personal o familiar. Con ello, se omite incluir el resguardo de otros derechos fundamentales que pueden involucrar información sensible sobre una persona que –por tener este carácter– no debe ser registrada ni menos difundida a terceros pues puede suponer afectación a otros derechos fundamentales, como la reserva de las convicciones ideológicas, religiosas o políticas; la orientación sexual; el estado de salud y enfermedades; o aspectos de índole privado cuya divulgación puede producir un tratamiento discriminatorio.

Al apreciar estas deficiencias en el texto del referido precepto constitucional, quienes elaboramos el proyecto de Código Procesal Constitucional –que a la postre fue aprobado como ley por el Congreso–, decidimos incluir, al regular los alcances del proceso de hábeas data –que protege este derecho–, una suerte de desarrollo o mayor precisión del contenido del derecho a la protección de los datos personales como una forma de suplir muchas de las carencias u omisiones antes señaladas. Así, en el artículo 61, numeral 2, del Código Procesal Constitucional se establece:

Artículo 61.- "El hábeas data procede en defensa de los derechos constitucionales reconocidos por los incisos 5) y 6) del Artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para: […]

2) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales".

Con esta norma se logró, según creemos, disipar diversas dudas sobre los alcances y el contenido de este derecho, abriendo mayores posibilidades para su ejercicio, operatividad y protección mediante el hábeas data. Es así que:

a) En vez de hacer referencia a "servicios informáticos", se alude a información o datos personales que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros.

b) Frente a la mención insuficiente al derecho de poder impedir el suministro o la difusión de los datos personales, el Código otorga también al titular los derechos a poder conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona.

c) El fundamento para la protección de este derecho, y para impedir que se suministre datos personales, no se circunscribe a la preservación de la intimidad personal y familiar, sino a prohibir la difusión de información de tipo sensible sobre el titular, que pueda afectar cualquier derecho constitucional.

Nuestro Tribunal Constitucional no ha sido ajeno a esta temática, realizando aportes para la mejor comprensión y protección del contenido y alcances del derecho a la protección de los datos personales y su control por el titular. Así, en los Fundamentos Jurídicos 2 al 4 de la sentencia recaída en el Expediente 4739-2007-PHD, de fecha 15 de octubre de 2007, sostuvo que:

"[e]l derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal.

Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen. […].

En este orden de ideas, el derecho a la autodeterminación informativa protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera «sensibles» y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos".

Partiendo de esta definición, podemos advertir que el derecho constitucional a la protección de los datos personales o de autodeterminación informativa cuenta con dos dimensiones: una negativa y otra positiva:

a) La dimensión "negativa" se traduce en la facultad que asiste al titular del derecho de prohibir el registro, la difusión y trasmisión de datos referidos a información de carácter personal "sensible".

b) La dimensión "positiva" implica la facultad del titular del derecho de poder controlar los datos concernientes a la propia persona. Dentro de este aspecto se encuentra el derecho de inspeccionar, verificar, actualizar y corregir los datos o informaciones referidas a su persona, así como el hacer cancelar toda aquella información referida a los datos personales sensibles que no debe ser registrada ni difundida.

III. LA LPDP: ALCANCES Y ÁMBITO DE APLICACIÓN

La Ley 29733, LPDP, tiene como objeto principal el regular los sistemas de almacenamiento, archivo, registro, sistematización y transmisión de datos

personales, contenidos en registros, bancos o bases de datos a cargo de entidades públicas o privadas, con el fin de proteger el derecho fundamental contenido en el artículo 2, inciso 6, de la Constitución. En consecuencia, se trata de una norma cuya naturaleza jurídica puede calificarse como de ley de desarrollo constitucional.

La LPDP contiene algunas **definiciones** referidas a aspectos básicos que son objeto de su regulación y tratamiento. Así, por ejemplo, en el numeral 2.4 se define como **datos personales** a "[t]oda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados". Esta definición es complementada en el reglamento (artículo 2, inciso 4), donde se señala que se trata de "[…] información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados".

En el numeral 2.1 de la LPDP, se define como **banco de datos personales** al "[c]onjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso". Estos bancos de datos personales, para efectos de la LPDP, pueden tener como titulares tanto a personas naturales o jurídicas de derecho privado como a entidades públicas.

Especial mención merece la referencia que se hace a los **datos sensibles**, que son definidos en el numeral 2.5 de la LPDP como "[d]atos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual".

A su vez, el reglamento (en su numeral 2.6) se refiere a los datos sensibles señalando que "[e]s aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad".

En cuanto a su ámbito de aplicación, la LPDP señala expresamente –en su artículo 3[1]– que será de aplicación a los datos personales contenidos, o que estén destinados a ser contenidos, en bancos de datos personales que sean administrados por entidades públicas o privadas en el territorio nacional. Asimismo, la norma agrega que tendrán especial protección los "datos sensibles". Este mismo artículo señala también los tipos de archivos, registros o bancos de datos donde **no resultará de aplicación la LPDP**, siendo éstos los siguientes:

a) Los datos personales contenidos en bancos de datos creados por personas naturales para su exclusivo uso privado, sea personal o familiar.

b) Los datos personales contenidos en bancos de datos administrados por entidades públicas, cuando su tratamiento sea necesario para el cumplimiento de sus funciones y competencias, siempre que estas se relacionen con asuntos vinculados a la defensa nacional, seguridad pública, y al desarrollo de actividades en materia penal para la investigación y represión del delito.

Nos parece acertada la exclusión del ámbito de aplicación de la LPDP de los bancos de datos creados por personas naturales, para su uso personal o familiar. Pero consideramos que la redacción de la ley y el reglamento –a este respecto– no es suficientemente precisa, pues hubiera sido preferible que se establezca expresamente que, dentro del uso para fines exclusivamente privados, deben entenderse comprendidos también los bancos de datos que se utilizan para el desarrollo de las actividades profesionales o laborales que realiza la persona que los ha creado. Pensamos, por ejemplo, en

[1] Artículo 3.- "Ámbito de aplicación

La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles.

Las disposiciones de esta Ley no son de aplicación a los siguientes datos personales:

1. A los contenidos o destinados a ser contenidos en bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.
2. A los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito".

los archivos o bases de datos confeccionados por un periodista, o en los que mantienen los profesionales (abogados, médicos, etcétera) como apoyo para el desempeño y ejercicio de su propia labor.

Conforme se puede apreciar, **la regla general** es que la LPDP será de aplicación a todos los archivos, registros, bancos o bases de datos personales que se establezcan en cualquier tipo de actividad económica, laboral, administrativa, científica, etcétera; sea que estén a cargo de entidades privadas o públicas, salvo que tengan como titular a personas naturales –para su uso privado– o a entidades públicas, únicamente cuando estén relacionados o sean necesarios para el cumplimiento de sus competencias institucionales, en materias como defensa nacional, seguridad pública, y acción penal de investigación y represión del delito.

Un ejemplo de archivos o registros de datos personales a cargo de entidades públicas y excluidos de la aplicación de la LPDP, son los relacionados con la Ley 27693[2], que creó la Unidad de Inteligencia Financiera del Perú [en adelante, UIF], cuyo artículo 3 dispone que la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones [en adelante, SBS] tiene la obligación de suministrar la información que le sea solicitada por la UIF, con el fin de prevenir el **lavado de dinero o de activos**. Consideramos que, atendiendo a lo dispuesto por el inciso 2 del artículo 3 de la LPDP, la información y los datos que posee la SBS en el Registro, vinculados al Sistema de Prevención del Lavado de Activos, se encuentran plenamente excluidos de los alcances y de la aplicación de la LPDP y su reglamento.

En similar situación de exclusión del ámbito de aplicación de la LPDP se encontrarían los archivos, registros o bancos de datos de instituciones públicas dedicadas a la preservación de la defensa nacional o seguridad pública, tales como los Ministerios de Defensa y del Interior, las fuerzas armadas y policiales, y los servicios de inteligencia.

Si bien mantener cierto grado de reserva en estos ámbitos resulta habitual y justificado, considero que hay que distinguir entre lo que supone la información de acceso público, que no está contemplada por la Constitución en estas materias, y la protección de datos personales, que concierne sólo a su titular. Porque podría ocurrir que dichas entidades estatales recojan y sistematicen indebidamente –en sus archivos y bancos de datos– información sobre datos personales sensibles e íntimos, entendiendo que ello resulta necesario para su tarea de preservación de la defensa nacional y seguridad pública.

Al quedar dichos registros fuera del ámbito de la LPDP, los titulares de dichos datos personales no podrán ejercer sus derechos de conocer el contenido de tal información, de corregir o actualizar lo inexacto o de hacer suprimir o impedir la difusión de lo indebidamente registrado. Ello nos parece bastante delicado, teniendo en cuenta que tal información supondría una invasión injustificada en la intimidad y privacidad de las personas, y que puede ser utilizada para fines de persecución política o ideológica, coacción o discriminación.

Al margen de ello, puede calificarse como positiva la opción acogida por la LPDP de incluir –dentro de su ámbito de aplicación y regulación– a un amplio conjunto de registros, bases y bancos de datos personales, a cargo de entidades públicas o privadas, con las exclusiones muy puntuales antes señaladas. Y ello porque así se puede brindar al titular de los datos personales acceso a innumerables registros y bases de datos, incluso de entidades privadas, así como el poder controlar que éstos no almacenen ni difundan información personal que podría estar vedada o restringida en su tratamiento.

Sin embargo, podrían formularse algunas dudas o reparos respecto a si esta extensa inclusión de diversos tipos de bancos de datos y registros dentro del ámbito de aplicación de la LPDP se adecúa a lo estipulado en la Constitución, así como si resulta lo más conveniente desde el punto de vista de su justificación y utilidad práctica.

En cuanto a la reflexión de índole constitucional, recordemos que el inciso 6 del artículo 2 de la Constitución, aunque inadecuado en su redacción como ya hemos afirmado, alude a los "servicios informáticos" como sujeto pasivo frente al que el titular de los datos personales puede accionar su derecho.

Desde una visión literal y estricta, esta expresión sugiere que las entidades públicas y privadas concernidas en esta materia serían las que cuentan con archivos, registros o bancos de datos donde se almacenan, sistematizan y difunden datos personales destinados o susceptibles de ser comunicados, consultados o de brindar información hacia terceros. Es decir, que tienen como finalidad dar servicios y acceso al público, sea en forma gratuita o a cambio de un pago por tal prestación.

Así lo entendió también el Código Procesal Constitucional, al regular las entidades respecto de las

[2] Publicada en el Diario Oficial "El Peruano" el 12 de abril de 2002.

cuales el titular de los datos personales podía interponer el hábeas data, señalando que tratándose de entidades privadas, abarcaba a los registros, archivos o bancos de datos que brindan acceso o servicios a terceros; es decir, a los que no están destinados al uso exclusivamente interno o privado de la entidad que los ha creado o administra.

No obstante, según ha dispuesto la LPDP, los registros o bancos de datos a cargo de entidades privadas –todos si su titular es una persona jurídica– están sujetos a la aplicación de la regulación de dicha ley, aunque se trate de registros o bases de datos personales destinados exclusivamente al uso interno, para los fines y actividades que desarrolla la entidad.

De este modo –por ejemplo–, cabe entender que cualquier empresa, universidad, club, sindicato, organización gremial o profesional, u otras entidades, por el simple hecho de contar con registros o bancos de datos personales referidos a sus trabajadores, proveedores, clientes, estudiantes asociados, afiliados –según sea el caso–, estarán también sujetas al cumplimiento del conjunto de exigencias y obligaciones contempladas en la LPDP; ello, aunque la creación y utilización de tales registros, archivos o bancos de datos personales, se restrinja al ámbito exclusivamente interno y para el desarrollo de los fines propios de la entidad.

Parecería claro, entonces, que la LPDP ha extendido e interpretado de manera amplia los alcances que la Constitución y el Código Procesal Constitucional contemplan respecto al tipo de entidades y sujetos pasivos objeto de control por el titular de los datos personales, que ya no se restringirían a los que están destinados a brindar servicios o acceso al público. La pregunta sería, no obstante, si con ello la LPDP podría ser acusada de haber incurrido en un "exceso" de tipo inconstitucional.

Pero también nos surgen algunas dudas sobre la utilidad práctica y conveniencia de esta tan amplia inclusión, en el ámbito de aplicación integral de la LPDP, de los registros y bancos de datos personales de entidades privadas constituidos para su uso exclusivamente interno. Nos parece atinada la inclusión de este tipo de registros y bancos de datos para permitir controlar que se sujeten a los principios contenidos en la LPDP, en temas tales como exclusión de datos de carácter reservado e información sensible, la indicación explícita de la finalidad u objeto del registro, la confidencialidad, el ejercicio de los derechos del titular de los datos, etcétera.

Sin embargo, seguramente pueden resultar excesivamente complejas, engorrosas u onerosas algunas otras exigencias generales que también impone la LPDP, tales como la obligación de registro del banco de datos ante la Autoridad Nacional de Protección de Datos Personales, el tener que contar con una organización que cuente con un titular del banco de datos y un encargado responsable de su tratamiento, las disposiciones en materia de mecanismos de seguridad y de orden técnico; ello, cuando se trata de entidades cuyos registros y bases de datos no están diseñados ni destinadas para suministrar ni trasmitir información a terceros.

En todo caso, pensamos que tal vez hubiera sido recomendable que la LPDP distinguiera entre ciertas exigencias y obligaciones aplicables a todo registro o banco de datos de entidades públicas o privadas, y otras aplicables sólo a aquellas entidades cuya actividad está concebida o destinada a brindar servicios e información sobre datos personales al público en general, o para ser trasmitidos a terceros.

IV. LA OBLIGACIÓN DE REGISTRO DE LOS BANCOS DE DATOS

El artículo 29 de la LPDP[3] establece que la creación, modificación y cancelación de bancos de datos personales, sean de administración de entidades públicas o privadas, se sujetarán a lo dispuesto en el reglamento, salvo lo que puedan establecer disposiciones especiales de otras leyes. Es importante resaltar que este precepto garantiza también la publicidad de la existencia de los bancos de datos, su finalidad, la identidad de su titular, etcétera; todo lo cual encontramos muy positivo y necesario.

Para facilitar y viabilizar la publicidad de la existencia y características de los bancos de datos personales, el artículo 34[4] de la LPDP establece la

[3] Artículo 29.- "Creación, modificación o cancelación de bancos de datos personales

La creación, modificación o cancelación de bancos de datos personales de administración pública y de administración privada se sujetan a lo que establezca el reglamento, salvo la existencia de disposiciones especiales contenidas en otras leyes. En todo caso, se garantiza la publicidad sobre su existencia, finalidad, identidad y el domicilio de su titular y, de ser el caso, de su encargado".

[4] Artículo 34.- "Registro Nacional de Protección de Datos Personales

Créase el Registro Nacional de Protección de Datos Personales como registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada, a nivel nacional, lo siguiente:

creación del Registro Nacional de Protección de Datos Personales, que estará a cargo de la **Autoridad Nacional de Protección de Datos Personales** [en adelante, ANPDP]. En dicho registro deberán **inscribirse** los bancos de datos a cargo de instituciones públicas o privadas. Sin embargo, en atención a lo dispuesto en el inciso 2 del artículo 34 de la LPDP, la ANPDP no podrá tener conocimiento del contenido de la base de datos que ante ella se registra, salvo la existencia de un procedimiento administrativo que lo habilite.

Ahora bien, cabe también tener presente lo establecido en la Quinta Disposición Complementaria Final de la LPDP[5], que impone la obligación de adecuar a la ley, dentro del plazo que dispone el reglamento, los bancos de datos personales creados con anterioridad a la vigencia de la LPDP, así como de declararlos e inscribirlos en el Registro Nacional de Protección de Datos Personales.

En consecuencia, todos los titulares de los bancos de datos que no se encuentren excluidos de los alcances y aplicación de la LPDP, estarán obligados a declararlos y registrarlos ante la ANPDP. El reglamento dispuso, en la primera de sus Disposiciones Complementarias Transitorias, que el plazo para la adecuación y registro de los bancos de datos existentes con anterioridad a la vigencia de la LPDP es de dos años, a contar desde la fecha de entrada en vigencia de dicho reglamento, por lo que se ha vencido hace poco.

V. LA EXIGENCIA DE OBTENER EL CONSENTIMIENTO, PREVIO Y EXPRESO, DEL TITULAR DE LOS DATOS PERSONALES PARA SU TRATAMIENTO

La LPDP contiene un conjunto de **principios rectores** que deben ser observados y cumplidos por los titulares y encargados de todo banco de datos, para efectos del registro y tratamiento de los datos personales. Entre estos principios, cabe destacar los de legalidad, consentimiento, finalidad, proporcionalidad, calidad y veracidad, seguridad, disposición de recursos administrativos y jurisdiccionales para la defensa y ejercicio del derecho, y protección adecuada.

El **principio de finalidad** (artículo 6 de la LPDP) implica que los datos personales que se recopilen estarán destinados a un fin explícito, determinado y lícito, sin que puedan utilizarse en otros fines; ello, salvo que sea para actividades científicas, estadísticas o históricas, y se respete procedimientos de anonimización o disociación respecto a la identidad del titular de los datos.

El artículo 5 de la LPDP establece el **principio del consentimiento**, que implica que para el tratamiento de los datos personales debe mediar la autorización otorgada por su titular. En el mismo sentido, el numeral 13.5 de la LPDP señala que "[l]os datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco".

En consecuencia, la regla general contenida en la LPDP es que para el tratamiento de los datos personales se deberá contar con el consentimiento y la autorización previa y expresa del titular de los mismos. El reglamento, en su artículo 16, contempla la posibilidad de que el titular de los datos personales pueda revocar el consentimiento que otorgó para el tratamiento de sus datos, sin que para ello requiera expresión de causa. Esta revocación no surtirá efectos retroactivos.

Tratándose de **datos personales sensibles**, el reglamento precisa que el consentimiento deberá

1. Los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean necesarios para el ejercicio de los derechos que corresponden a los titulares de datos personales, conforme a lo dispuesto en esta Ley y en su reglamento.

   El ejercicio de esta función no posibilita el conocimiento del contenido de los bancos de datos personales por parte de la Autoridad Nacional de Protección de Datos Personales, salvo procedimiento administrativo en curso.
2. Las autorizaciones emitidas conforme al reglamento de la presente Ley.
3. Las sanciones, medidas cautelares o correctivas impuestas por la Autoridad Nacional de Protección de Datos Personales conforme a esta Ley y a su reglamento.
4. Los códigos de conducta de las entidades representativas de los titulares o encargados de bancos de datos personales de administración privada.
5. Otros actos materia de inscripción conforme al reglamento.

   Cualquier persona puede consultar en el Registro Nacional de Protección de Datos Personales la existencia de bancos de datos personales, sus finalidades, así como la identidad y domicilio de sus titulares y, de ser el caso, de sus encargados".

[5] Quinta Disposición Complementaria Final.- "Bancos de datos personales preexistentes

Los bancos de datos personales creados con anterioridad a la presente Ley y sus respectivos reglamentos deben adecuarse a esta norma dentro del plazo que establezca el reglamento. Sin perjuicio de ello, sus titulares deben declararlos ante la Autoridad Nacional de Protección de Datos Personales, con sujeción a lo dispuesto en el artículo 29".

ser otorgado por escrito y en forma indubitable (artículo 14), correspondiendo la prueba de su obtención al titular del banco de datos o al responsable de su tratamiento. Sin embargo, la propia LPDP contiene algunas excepciones a esta regla general sobre la necesidad de obtener el consentimiento previo del titular para el tratamiento de sus datos personales.

Así, en su artículo 14 se enumeran diversos casos que quedan exceptuados de esta exigencia[6]. Pueden mencionarse, entre otros supuestos de exclusión contenidos en dicho artículo, ejemplos como los siguientes: cuando la recopilación y transferencia de datos es realizada por una entidad pública para el cumplimiento de sus funciones y competencias, cuando los datos personales se destinan a bancos de datos de acceso del público, cuando los datos personales se refieren a la solvencia patrimonial o de crédito, etcétera.

De esta norma, podemos apreciar –por ejemplo– que registros tales como la Central de Riesgos de la SBS, al ser accesible a cualquier persona interesada –previo pago de una tarifa– y tener como finalidad la de contar con información consolidada y clasificada sobre los deudores de las empresas, los riesgos por endeudamientos financieros crediticios en el país y en el exterior, los riesgos comerciales, etcétera; se encuentran claramente excluidos de la obligación de obtener el consentimiento previo y expreso del titular de los datos personales. Ello, porque su naturaleza y finalidad corresponden a un registro que contiene datos personales accesibles para el público, que están referidos a determinar o evaluar la solvencia patrimonial y de crédito de una persona.

La LPDP, en su numeral 13.8, se refiere al **tratamiento de datos personales relativos a la comisión de infracciones penales o administrativas**, señalando que sólo puede ser efectuado por las entidades públicas competentes, salvo convenio de encargo de gestión conforme a la Ley 27444, Ley del Procedimiento Administrativo General[7]. Cuando se haya producido la cancelación de los antecedentes penales, judiciales, policiales y administrativos, estos datos no pueden ser suministrados, salvo que sean requeridos por el Poder Judicial o el Ministerio Público.

VI. LOS DERECHOS DEL TITULAR DE LOS DATOS PERSONALES

A diferencia de la norma constitucional, que sólo menciona el derecho del titular de los datos personales a impedir el suministro de información que afecte su intimidad personal o familiar, ya dijimos que el Código Procesal Constitucional señala expresamente, como derechos del titular, el acceder y conocer los datos registrados sobre su persona, el poder rectificarlos, actualizarlos o hacerlos suprimir. La LPDP desarrolla y complementa, con mayor detalle y amplitud, los alcances de

6 Artículo 14.- "Limitaciones al consentimiento para el tratamiento de datos personales

No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:

1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de datos personales.
10. Otros establecidos por ley, o por el reglamento otorgado de conformidad con la presente Ley".

7 Publicada en el Diario Oficial "El Peruano" el 11 de abril de 2001.

estos derechos, que sólo podrán ser ejercidos por la persona titular de los datos personales o por su representante.

El artículo 18 de la LPDP establece que el titular de los datos personales tiene **derecho a ser informado**, con anterioridad a la recopilación de sus datos, sobre la finalidad del tratamiento de éstos, sus posibles destinatarios, la identificación del banco de datos donde se almacenarán y su titular, el carácter obligatorio o facultativo de la respuesta sobre datos sensibles, etcétera. En el artículo 19 se regula el **derecho de acceso** del titular de los datos personales, pudiendo este solicitar y obtener la información que sobre él se encuentra registrada o es objeto de tratamiento, la forma y motivos por los que sus datos fueron recopilados, así como las transferencias de los mismos (efectuadas o que se prevén realizar).

En el artículo 20 de la LPDP se regulan los derechos del titular de los datos personales a realizar la **actualización, inclusión, rectificación y supresión** de éstos, cuando: sean inexactos, incompletos, falsos, errados; haya dejado de ser necesaria la finalidad para la cual se recopilaron; o haya vencido el plazo establecido para su tratamiento. Señala también la obligación del encargado del registro o banco de datos de informar de esta modificación a quienes se haya transmitido anteriormente los datos.

El artículo 21 refiere el derecho del titular de los datos a **impedir que sean suministrados**, cuando con ello se afecten sus derechos fundamentales; mientras que en el artículo 22 se reconoce su derecho a oponerse al tratamiento de sus datos personales, cuando no se haya prestado su consentimiento o existan motivos fundados o legítimos de una situación personal concreta, a menos que la ley disponga otra cosa.

En caso de que el titular o el encargado del banco de datos o registro deniegue el ejercicio de alguno de los derechos reconocidos al titular de los datos personales, la LPDP habilita su **derecho a obtener tutela** por las vías administrativa o judicial (artículo 24). Así, podrá interponer un reclamo administrativo ante la ANPDP, o un hábeas data ante el Poder Judicial. El artículo 25 de la LPDP reconoce el derecho del titular de los datos personales a obtener una indemnización, en caso de incumplimiento de dicha ley o por los perjuicios que le ocasione el titular o el encargado del banco de datos o un tercero.

VII. LA ANPDP

Según dispone el artículo 32 de la LPDP, la ANPDP es el Ministerio de Justicia (hoy, Ministerio de Justicia y Derechos Humanos), a través de la Dirección Nacional de Justicia. A dicho órgano compete velar por el cumplimiento del objeto y las obligaciones establecidos en la LPDP y su reglamento, así como ejercer la potestad sancionadora con atribuciones coactivas.

En el artículo 33 de la LPDP se enumera un amplio conjunto de funciones de la ANPDP, que comprenden aspectos tales como la representación internacional del país en este campo, la supervisión y fiscalización del cumplimiento de la normativa de esta materia, la administración del Registro Nacional de Protección de Datos Personales, la emisión de opiniones técnicas y absolución de consultas, el conocimiento y resolución de los procedimientos administrativos por reclamos de los titulares de los datos personales, el ejercicio de la potestad sancionadora, etcétera.

Si bien la ANPDP es una entidad pública de carácter administrativo, cuya existencia no emana de la Constitución sino de una ley, resulta bastante discutible la justificación y conveniencia de la decisión de la LPDP de atribuirle este rol a una entidad subalterna ubicada al interior de la estructura del Ministerio de Justicia. Y no sólo porque ello puede afectar sus niveles reales de autonomía, aspecto ciertamente delicado por tratarse de una instancia que debe controlar el respeto de un derecho constitucional como la protección de los datos personales, sino porque la Dirección a la que se integra tiene un conjunto recargado de funciones ordinarias y limitaciones operativas o presupuestales que dificultan su adecuado desarrollo y proyección.

En nuestro país existen diversos organismos administrativos que cumplen funciones de control y supervisión, fiscalización o de orden técnico especializado, cuya autonomía funcional no sólo se encuentra legalmente consagrada sino que ésta se efectiviza al ubicarlos fuera de la estructura interna de los ministerios, aunque se encuentren adscritos a un sector determinado de la Administración Pública. Pensemos, por ejemplo, en entidades como el Indecopi[8], en materia de defensa de la competencia económica y protección de la propiedad intelectual, o del OEFA[9], como organismo de fiscalización ambiental, que no están insertas dentro de la estructura interna de un ministerio. Incluso,

[8] Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.

[9] Organismo de Evaluación y Fiscalización Ambiental.

tratándose del sector Justicia, la Superintendencia Nacional de los Registros Públicos [SUNARP], cuenta con un estatus de organismo autónomo adscrito a dicho Ministerio.

Sin duda, las funciones de la ANPDP no son menos relevantes y delicadas que las que corresponden a los organismos antes mencionados, por lo que no resulta justificada ni conveniente la decisión adoptada por la LPDP de colocar a la ANPDP en una instancia dentro de la estructura interna del Ministerio de Justicia.

Si nos atenemos a lo establecido para instituciones similares en otros países –como en España o en México o en el caso de Latinoamérica– y al papel que está llamado a cumplir la ANPDP, consideramos que debe revisarse la ubicación dentro del aparato estatal y del Poder Ejecutivo que le ha asignado la LPDP, a fin de dotarla y garantizarle adecuados niveles de autonomía funcional y proyección institucional, acordes con los estándares internacionales.

VIII. REFLEXIÓN FINAL

La consagración de la protección de los datos personales como un derecho fundamental resulta un suceso relativamente reciente en el ámbito constitucional nacional y comparado. Su surgimiento y reconocimiento constitucional supuso una autonomización del derecho a la intimidad personal, fuertemente influenciado por el desarrollo vertiginoso de las nuevas tecnologías de la información. Su protección y regulación se hace muy importante para garantizar que el titular de este derecho pueda tener mayor nivel de control y determinación autónoma sobre los datos personales e información referida a su persona, que se registran, sistematizan y transmiten, muchas veces sin su conocimiento.

Por ello, la expedición de la LPDP y su reglamento, más allá de la demora producida en su aprobación, son un paso muy positivo para el desarrollo y aplicación del derecho estipulado en el inciso 6 del artículo 2 de la Constitución, que seguramente contribuirá a avanzar en la mejor regulación y protección de este derecho fundamental de la persona.

En este breve trabajo, hemos querido dar cuenta de algunos aspectos relevantes contenidos en dichas normas, formulando también algunas dudas y observaciones al respecto. Consideramos que lo prudente y aconsejable es dar un tiempo a la aplicación de tales normas, al cabo del cual corresponderá realizar una evaluación de su funcionamiento y de la experiencia concreta. Ello permitirá determinar si algunas de nuestras atingencias o reparos se verifican efectivamente o no, así como detectar posibles vacíos o deficiencias que deberán ser corregidas.