Proyecto de Ley N° 4079/2009-PE

CONGRESO DE LA REPÚBLICA
AREA DE TRAMITE DOCUMENTARIO
9 - JUN 2010
RECIBIDO
Firma: Hora: 20:00

"Decenio de las Personas con Discapacidad en el Perú"
"Año de la consolidación económica y social del Perú"

Lima, 09 de junio de 2010

OFICIO N° 128-2010-PR

Señor Doctor
LUIS ALVA CASTRO
Presidente del Congreso de la República
Presente.-

Tenemos el agrado de dirigirnos a usted, de conformidad con lo dispuesto por el artículo 107° de la Constitución Política del Perú, a fin de someter a consideración del Congreso de la República, con el voto aprobatorio del Consejo de Ministros, el proyecto de Ley de Protección de Datos Personales.

Mucho estimaremos que se sirva disponer su trámite con el carácter de URGENTE, según lo establecido por el Artículo 105° de la Constitución Política del Perú.

Sin otro particular, hacemos propicia la oportunidad para renovarle los sentimientos de nuestra estima y consideración.

Atentamente,

ALAN GARCÍA PÉREZ
Presidente Constitucional de la República

JAVIER VELÁSQUEZ QUESQUÉN
Presidente del Consejo de Ministros

CONGRESO DE LA REPUBLICA
Lima, 17 de junio del 2010
Según la consulta realizada, de conformidad con el Artículo 77° del Reglamento del Congreso de la República: pase la Proposición N° 4079 Para su estudio y dictamen, a la (s) Comisión (es) de Justicia y Derechos Humanos.

JOSÉ ABANTO VALDIVIESO
Oficial Mayor (e)
CONGRESO DE LA REPÚBLICA

Proyecto de Ley

LEY DE PROTECCIÓN DE DATOS PERSONALES

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1°.- Objeto

La presente Ley tiene por objeto garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2° inciso 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto a los demás derechos fundamentales que en ella se reconocen, particularmente los derechos al honor, buena reputación, intimidad, voz e imagen propias.

Artículo 2°.- Definiciones

Para todos los efectos de la presente Ley, se entenderá por:

2.1 Banco de datos personales.- Conjunto 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.

2.2 Banco de datos personales de administración privada.- Banco de datos personales cuya titularidad corresponde a una persona natural o a una persona jurídica de derecho privado, en cuanto el banco no se encuentre estrictamente vinculado al ejercicio de potestades de derecho público.

2.3 Banco de datos personales de administración pública.- Banco de datos personales cuya titularidad corresponde a una entidad pública.

2.4 Datos personales.- Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que puedan ser razonablemente utilizados.

2.5 Datos sensibles.- Datos personales constituidos por los datos biométricos, datos referidos al origen racial y étnico; opiniones o convicciones políticas, religiosas, filosóficas o morales; hábitos personales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

2.6 Encargado del banco de datos personales.- Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra, realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.

2.7 Entidad pública.- Entidad comprendida en el artículo I del Título Preliminar de la Ley Nº 27444, Ley del Procedimiento Administrativo General o la que haga sus veces.

2.8 Flujo transfronterizo de datos personales.- Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que éstos se encuentren, los medios por los cuales se efectuó la transferencia, ni el tratamiento que reciban.

2.9 Fuentes accesibles por el público.- Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles por el público serán determinadas en el reglamento.

2.10 Persona jurídica de derecho privado.- Para efectos de esta Ley, la persona jurídica no comprendida en los alcances del artículo I del Título Preliminar de la Ley Nº 27444, Ley del Procedimiento Administrativo General.

2.11 Procedimiento de anonimización.- Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de éstos. El procedimiento es irreversible.

2.12 Procedimiento de disociación.- Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de éstos. El procedimiento es reversible.

2.13 Titular de datos personales.- Persona natural a quien corresponden los datos personales.

2.14 Titular del banco de datos personales.- Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de éstos y las medidas de seguridad.

2.15 Transferencia de datos personales.- Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.

2.16 Tratamiento de datos personales.- Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.

El reglamento de esta Ley podrá establecer otras definiciones y/o realizar un mayor desarrollo de las existentes.

Artículo 3°.- Ámbito de aplicación

Esta 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 realice en el territorio nacional. Son objeto de especial protección los datos sensibles.

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

3.1 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.

3.2 A los contenidos o destinados a ser contenidos en bancos de datos de administración pública, sólo 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, el desarrollo de actividades en materia penal para la investigación y represión del delito.

TÍTULO II

PRINCIPIOS RECTORES

Artículo 4°.- Principio de legalidad

El tratamiento de los datos personales se hará conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.

Artículo 5°.- Principio de consentimiento

Para el tratamiento de los datos personales deberá mediar el consentimiento de su titular.

Artículo 6°.- Principio de finalidad

Los datos personales deberán ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no deberá extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Artículo 7°.- Principio de proporcionalidad

Todo tratamiento de datos personales deberá ser adecuado, relevante y no excesivo a la finalidad para la que éstos hubiesen sido recopilados.

Artículo 8°.- Principio de calidad

Los datos personales que vayan a ser tratados deberán ser veraces, exactos y en la medida de lo posible actualizados, necesarios, pertinentes y adecuados con la finalidad para la que fueron recopilados. Deberán conservarse de forma tal que se garantice su seguridad y sólo por el tiempo necesario para cumplir con la finalidad del tratamiento.

Artículo 9°.- Principio de seguridad

El titular del banco de datos personales y el encargado de su tratamiento deberán adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deberán ser

apropiadas y acordes al tratamiento que se vaya a efectuar y a la categoría de datos personales de que se trate.

Artículo 10°.- Principio de disposición de recurso

Todo titular de datos personales deberá contar con las vías administrativas y/o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando éstos sean vulnerados por el tratamiento de sus datos personales.

Artículo 11°.- Principio de nivel de protección adecuado

En el caso de flujo transfronterizo de datos personales, el país destinatario deberá contar con un nivel suficiente de protección para los datos personales que se vayan a tratar, o por lo menos comparable al previsto por esta Ley.

El ámbito suficiente de protección del país destinatario deberá abarcar por lo menos la consignación y el respeto de los principios rectores de la protección de datos personales objeto de este Título y un sistema efectivo de garantías.

Artículo 12°.- Valor de los principios

La actuación de los titulares y encargados de los bancos de datos personales y, en general, de todos los que intervengan en relación a datos personales, deberá ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa.

Los principios rectores señalados servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia.

TÍTULO III

TRATAMIENTO DE DATOS PERSONALES

Artículo 13°.- Alcances del tratamiento

13.1 El tratamiento de datos personales debe realizarse en pleno respeto de los derechos fundamentales de sus titulares y de los derechos que esta Ley les confiere. Igual regla rige para su utilización por terceros.

13.2 Las limitaciones al ejercicio del derecho fundamental a la protección de datos personales sólo pueden ser establecidas por ley, respetando su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos.

13.3 Mediante reglamento se dictarán medidas especiales para el tratamiento de los datos personales de los niños y de los adolescentes, así como para la protección y garantía de sus derechos. Para el ejercicio de los derechos que esta Ley reconoce, los niños y adolescentes actuarán a través de sus representantes legales, pudiendo el reglamento determinar las excepciones aplicables, de ser el caso, teniendo en cuenta para ello el interés superior del niño y del adolescente.

13.4 Las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter o uso privado, sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez o con autorización de su titular, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. Los datos personales obtenidos con violación de este precepto carecen de efecto legal.

13.5 Los datos personales sólo podrán ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento deberá ser previo, informado, expreso e inequívoco.

13.6 En el caso de datos sensibles, el consentimiento para efectos de su tratamiento además deberá efectuarse por escrito. Aun cuando no mediara el consentimiento del titular, el tratamiento de datos sensibles podrá efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público.

13.7 El titular de datos personales podrá revocar su consentimiento en cualquier momento debiendo sustentar su solicitud cuando corresponda, observando al efecto los mismos requisitos que con ocasión de su otorgamiento.

13.8 El tratamiento de datos personales relativos a la comisión de infracciones penales o administrativas sólo puede ser efectuado por las entidades públicas competentes, salvo convenio de encargo de gestión conforme a la Ley Nº 27444, Ley del Procedimiento Administrativo General o la que haga sus veces. Cuando se haya producido la cancelación de los antecedentes penales, judiciales, policiales y administrativos, estos datos no podrán ser suministrados salvo que sean requeridos por el Poder Judicial o el Ministerio Público, conforme a Ley.

13.9 La comercialización de datos personales contenidos o destinados a ser contenidos en bancos de datos personales se sujeta a lo dispuesto en el reglamento de la Ley.

Proyecto de Ley

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

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

14.1 Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.

14.2 Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles por el público.

14.3 Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a Ley.

14.4 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 N° 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.

14.5 Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte.

14.6 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 por establecimientos de salud o por profesionales de 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 o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.

14.7 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 deberán guardar relación con el propósito a que se circunscriban sus actividades, no pudiendo ser transferidos sin consentimiento de aquéllos.

14.8 Cuando se hubiera aplicado un procedimiento de anonimización o disociación.

14.9 Otros establecidos por Ley.

Artículo 15°.- Flujo transfronterizo de datos personales

El titular y el encargado del banco de datos personales podrán realizar el flujo transfronterizo de datos personales sólo si los destinatarios mantienen niveles de protección adecuados conforme a la presente Ley. La Autoridad Nacional de Protección de Datos Personales supervisará el cumplimiento de esta exigencia.

No se aplica lo dispuesto en el párrafo anterior en los siguientes casos:

15.1 Acuerdos en el marco de tratados internacionales sobre la materia en los cuales la República del Perú sea parte.

15.2 Cooperación judicial internacional.

15.3 Cooperación internacional entre organismos de inteligencia para la lucha contra el terrorismo, tráfico ilícito de drogas, lavado de activos, corrupción, trata de personas y otras formas de criminalidad organizada.

15.4 Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte.

15.5 Cuando se trate de transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la Ley aplicable.

15.6 Cuando el flujo transfronterizo de datos personales se realice para la prevención, diagnóstico o tratamiento médico o quirúrgico de su titular; o cuando sea necesario para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.

15.7 Cuando el titular de los datos personales haya dado su consentimiento previo, informado, expreso e inequívoco.

15.8 Otros que establezca el reglamento de la presente Ley.

Artículo 16°.- Seguridad

Para fines del tratamiento de datos personales, el titular del banco de datos personales deberá adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Los requisitos y condiciones que deberán reunir los bancos de datos personales en materia de seguridad serán establecidos por la Autoridad Nacional de Protección de Datos Personales.

Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo.

Artículo 17°.- Confidencialidad

El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsistirá aún después de finalizadas las relaciones con el titular del banco de datos personales.

El obligado podrá ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública; sin perjuicio del derecho a guardar el secreto profesional.

TÍTULO IV

DERECHOS DEL TITULAR DE DATOS PERSONALES

Artículo 18°.- Derecho de información

El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes serán o podrán ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conservarán sus datos personales; y, la posibilidad de ejercer los derechos que la ley le concede.

Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo podrán satisfacerse mediante la publicación de políticas de privacidad, las que deberán ser fácilmente accesibles e identificables.

Artículo 19°.- Derecho de acceso

El titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

Artículo 20°.- Derecho de actualización, inclusión, rectificación y supresión

El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando éstos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

Si sus datos personales hubieran sido transferidos previamente, el encargado del banco de datos personales deberá comunicar la actualización, inclusión, rectificación y/o supresión a quien se hayan transferido, en el caso que se mantenga el tratamiento por este último, quien deberá también proceder a la actualización, inclusión, rectificación y/o supresión, según corresponda.

Durante el proceso de actualización, inclusión, rectificación y/o supresión de datos personales, el encargado del banco de datos personales dispondrá su bloqueo, quedando impedido de permitir que terceros accedan a ellos.

La supresión de datos personales contenidos en bancos de datos personales de administración pública se sujeta a lo dispuesto en el artículo 21° del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública o la que haga sus veces.

Artículo 21°.- Derecho a impedir el suministro

El titular de datos personales tiene derecho a impedir que éstos sean suministrados, especialmente cuando ello afecte sus derechos fundamentales.

Artículo 22°.- Derecho de oposición

Siempre que por ley no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada, el titular o el encargado del banco de datos personales, según corresponda, deberá proceder a su supresión, conforme a ley.

Proyecto de Ley

Artículo 23°.- Derecho al tratamiento objetivo

El titular de datos personales tiene derecho a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad, salvo que ello ocurra en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo a ley, sin perjuicio de la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo.

Artículo 24°.- Derecho a la tutela

En caso el titular o el encargado del banco de datos personales deniegue al titular de datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta Ley, éste podrá recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación, o al Poder Judicial para efectos de la correspondiente acción de habeas data.

El procedimiento a seguir ante la Autoridad Nacional de Protección de Datos Personales se sujeta a lo dispuesto en los artículos 219° y siguientes de la Ley N° 27444, Ley del Procedimiento Administrativo General o la que haga sus veces.

La resolución de la Autoridad Nacional de Protección de Datos Personales agota la vía administrativa y habilita a la imposición de las sanciones administrativas previstas en el artículo 39° de esta Ley. El reglamento determinará las instancias correspondientes.

Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa.

Artículo 25°.- Derecho a ser indemnizado

El titular de datos personales que sea afectado como consecuencia del incumplimiento de la presente Ley por el titular o por el encargado del banco de datos personales o por terceros, tiene derecho a obtener la indemnización correspondiente conforme a ley.

Artículo 26°.- Gratuidad

No se exigirá contraprestación alguna al titular de datos personales por el ejercicio de los derechos contemplados en los artículos 19°, 20°, 21°, 22° y 23° de esta Ley, salvo en los casos que establezca el reglamento.

Artículo 27°.- Limitaciones

Los titulares y encargados de los bancos de datos de administración pública pueden denegar el ejercicio de los derechos de acceso, actualización, inclusión, rectificación, supresión y oposición por razones fundadas en la protección de derechos e intereses de terceros o cuando ello pueda 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 verificación de infracciones administrativas, o cuando así lo disponga la ley.

TÍTULO V

OBLIGACIONES DEL TITULAR Y DEL ENCARGADO DEL BANCO DE DATOS PERSONALES

Artículo 28°.- Obligaciones

El titular y el encargado del banco de datos personales, según sea el caso, tienen las siguientes obligaciones:

28.1 Efectuar el tratamiento de datos personales, sólo previo consentimiento informado, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa.

28.2 No recopilar datos personales por medios fraudulentos, desleales o ilícitos.

28.3 Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido.

28.4 No utilizar los datos personales objeto de tratamiento para finalidades distintas de aquéllas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación.

28.5 Almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular.

28.6 Suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto.

28.7 Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.

28.8 Proporcionar a la Autoridad Nacional de Protección de Datos Personales la información relativa al tratamiento de datos personales que ésta le requiera y permitirle el acceso a los bancos de datos personales que administra, para el ejercicio de sus funciones.

28.9 Otras establecidas en esta Ley y en su reglamento.

TÍTULO VI
BANCOS DE DATOS PERSONALES

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 sujetarán a lo que establezca el reglamento, garantizándose la publicidad sobre su existencia, finalidad y la identidad y domicilio de su titular y, de ser el caso, de su encargado.

Artículo 30°.- Prestación de servicios de tratamiento de datos personales

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 o convenio celebrado, ni ser transferidos a otras personas, ni aun para su conservación.

Una vez ejecutada la prestación materia del contrato o del convenio, según el caso, los datos personales tratados deberán ser suprimidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrán conservar con las debidas condiciones de seguridad, hasta por el plazo que determine el reglamento de la presente Ley.

Artículo 31°.- Códigos de conducta

Las entidades representativas de los titulares o encargados de bancos de datos personales de administración privada podrán elaborar códigos de conducta, 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 rectores establecidos en la presente Ley.

TÍTULO VII

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

Artículo 32°.- Órgano competente y régimen jurídico

El Ministerio de Justicia, a través de la Dirección Nacional de Justicia, es la Autoridad Nacional de Protección de Datos Personales. Para el adecuado desempeño de sus funciones podrá crear oficinas en todo el país.

La Autoridad Nacional de Protección de Datos Personales se rige por lo dispuesto en esta Ley, en su reglamento y en los artículos pertinentes del Reglamento de Organización y Funciones del Ministerio de Justicia.

Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la presente Ley y de su reglamento. Para tal efecto goza de potestad sancionadora, de conformidad con la Ley N° 27444, Ley del Procedimiento Administrativo General o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley N° 26979, Ley de Procedimiento de Ejecución Coactiva o la que haga sus veces.

La Autoridad Nacional de Protección de Datos Personales deberá presentar periódicamente un informe sobre sus actividades al Ministro de Justicia.

Artículo 33°.- Funciones

La Autoridad Nacional de Protección de Datos Personales ejercerá las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:

33.1 Representar al país ante las instancias internacionales en materia de protección de datos personales.

33.2 Cooperar con las autoridades extranjeras de protección de datos personales para el cumplimiento de sus competencias y generar mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse debido auxilio mutuo cuando se requiera.

33.3 Administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales.

33.4 Publicitar, a través del Portal Institucional, la relación actualizada de bancos de datos personales de administración pública y privada.

33.5 Promover campañas de difusión y promoción sobre la protección de datos personales.

33.6 Promover y fortalecer una cultura de protección de los datos personales de los niños y adolescentes.

33.7 Coordinar la inclusión de información sobre la importancia de la vida privada y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo, la capacitación de los docentes en estos temas.

33.8 Emitir autorizaciones, cuando corresponda, conforme al reglamento de la presente Ley.

33.9 Absolver consultas sobre protección de datos personales y el sentido de las normas vigentes sobre tal materia, particularmente sobre las que ella hubiera emitido.

33.10 Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la que será vinculante.

33.11 Emitir las directivas que correspondan para la mejor aplicación de lo previsto en la presente Ley y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados.

33.12 Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales.

33.13 Celebrar convenios de cooperación interinstitucional y/o internacional con la finalidad de velar por los derechos de las personas en materia de protección de datos personales que son tratados dentro y fuera del territorio nacional.

33.14 Atender solicitudes en interés particular del administrado o general de la colectividad, así como solicitudes de información.

33.15 Conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares y/o correctivas que establezca el reglamento.

33.16 Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores.

33.17 Obtener de los titulares de los bancos de datos personales la información que estime necesaria para el cumplimiento de las normas sobre protección de datos personales y el desempeño de sus funciones.

33.18 Supervisar el tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales y, en caso de ilegalidad, disponer las acciones que correspondan conforme a Ley.

33.19 Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares y/o correctivas que establezca el reglamento.

33.20 Las demás funciones que le asignen la presente Ley y su reglamento.

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:

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

34.2 Las autorizaciones emitidas conforme al reglamento de la presente Ley.

34.3 Las sanciones, medidas cautelares y /o correctivas impuestas por la Autoridad Nacional de Protección de Datos Personales conforme a esta Ley y a su reglamento.

34.4 Los códigos de conducta de las entidades representativas de los titulares o encargados de bancos de datos personales de administración privada.

34.5 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.

Artículo 35°.- Confidencialidad

El personal de la Autoridad Nacional de Protección de Datos Personales está sujeto a la obligación de guardar confidencialidad sobre los datos personales que conozca con motivo de sus funciones. Esta obligación subsistirá aún después de finalizada toda relación con dicha Autoridad Nacional, bajo responsabilidad.

Artículo 36°.- Recursos

Son recursos de la Autoridad Nacional de Protección de Datos Personales los siguientes:

36.1 Las tasas por concepto de derecho de trámite de los procedimientos administrativos y servicios de su competencia.

36.2 Los montos que recaude por concepto de multas.

36.3 Los recursos provenientes de la cooperación técnica internacional no reembolsable.

36.4 Los legados y donaciones que reciba.

36.5 Los recursos que se le transfieran conforme a Ley.

Los recursos de la Autoridad Nacional de Protección de Datos Personales serán destinados a financiar los gastos necesarios para el desarrollo de sus operaciones y para su funcionamiento.

TÍTULO VIII
INFRACCIONES Y SANCIONES ADMINISTRATIVAS

Artículo 37°.- Procedimiento sancionador

El procedimiento sancionador se inicia de oficio por la Autoridad Nacional de Protección de Datos Personales o por denuncia de parte, ante la presunta comisión

de actos contrarios a lo dispuesto en la presente Ley o en su reglamento, sin perjuicio del procedimiento seguido en el marco de lo dispuesto en el artículo 24° de esta Ley.

Las Resoluciones de la Autoridad Nacional de Protección de Datos Personales agotan la vía administrativa.

Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa.

Artículo 38°.- Infracciones

Constituye infracción sancionable toda acción u omisión que contravenga las disposiciones de la presente Ley o de su reglamento. Las infracciones se califican como leves, graves y muy graves. La tipificación de las infracciones, graduación del monto de las multas y el procedimiento para su aplicación se efectuará en el reglamento de la presente Ley.

Artículo 39°.- Sanciones administrativas

En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales podrá aplicar las siguientes multas:

39.1 Las infracciones leves serán sancionadas con una multa mínima de 0.5 (cero punto cinco) Unidades Impositivas Tributarias hasta de 5 (cinco) Unidades Impositivas Tributarias.

39.2 Las infracciones graves serán sancionadas con multa de más de 5 (cinco) Unidades Impositivas Tributarias hasta 50 (cincuenta) Unidades Impositivas Tributarias.

39.3 Las infracciones muy graves serán sancionadas con multa de más de 50 (cincuenta) Unidades Impositivas Tributarias hasta 100 (cien) Unidades Impositivas Tributarias.

En ningún caso la multa impuesta podrá exceder el 10 % (diez por ciento) de los ingresos brutos anuales que hubiera percibido el presunto infractor durante el ejercicio anterior.

La Autoridad Nacional de Protección de Datos Personales determinará la infracción cometida y el monto de la multa imponible mediante Resolución debidamente motivada. Para la graduación del monto de las multas se tomarán en cuenta los criterios establecidos en el artículo 230° numeral 3) de la Ley N° 27444, Ley del Procedimiento Administrativo General o la que haga sus veces.

La imposición de la multa se efectuará sin perjuicio de las sanciones disciplinarias sobre el personal de las entidades públicas en los casos de bancos de datos personales de administración pública, así como de la indemnización por daños y perjuicios y de las sanciones penales a que hubiera lugar.

Artículo 40°.- Multas coercitivas

En aplicación de lo dispuesto en el artículo 199° de la Ley N° 27444, Ley del Procedimiento Administrativo General o la que haga sus veces, la Autoridad Nacional de Protección de Datos Personales podrá imponer multas coercitivas por un monto que no supere las diez (10) UIT, frente al incumplimiento de las obligaciones accesorias a la sanción, impuestas en el procedimiento sancionador. Las multas coercitivas se impondrán una vez vencido el plazo de cumplimiento.

La imposición de las multas coercitivas no impide el ejercicio de otro medio de ejecución forzosa conforme a lo dispuesto en el artículo 196° de la Ley N° 27444.

El reglamento de la ley regulará lo concerniente a la aplicación de las multas coercitivas.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- Reglamento

El reglamento de la presente Ley será aprobado por Decreto Supremo con refrendo del Ministro de Justicia.

Para la elaboración del proyecto de reglamento, se constituirá una Comisión Multisectorial, la que será presidida por la Autoridad Nacional de Protección de Datos Personales. El proyecto de reglamento será elaborado en un plazo máximo de ciento veinte (120) días hábiles, a partir de la instalación de la Comisión Multisectorial, lo que deberá ocurrir en un plazo no mayor de 15 (quince) días hábiles.

Segunda.- Directiva de seguridad

La Autoridad Nacional de Protección de Datos Personales elaborará la directiva de seguridad de la información administrada por los bancos de datos personales en un plazo no mayor de ciento veinte (120) días hábiles. En tanto se apruebe y rija la referida directiva, se mantendrán vigentes las disposiciones sectoriales sobre la materia.

Tercera.- Adecuación de documentos de gestión y de Texto Único de Procedimientos Administrativos del Ministerio de Justicia

Estando a la creación de la Autoridad Nacional de Protección de Datos Personales, en un plazo máximo de ciento veinte (120) días hábiles el Ministerio de Justicia elaborará las modificaciones pertinentes en sus documentos de gestión y en su Texto Único de Procedimientos Administrativos.

Cuarta.- Adecuación y propuesta de normativa específica sobre datos personales

Durante un plazo no mayor de 60 (sesenta) días hábiles, bajo la orientación y supervisión de la Autoridad Nacional de Protección de Datos Personales, las entidades públicas competentes revisarán la normativa que verse sobre datos personales y elaborarán las propuestas necesarias para su adecuación a lo dispuesto en esta Ley. En caso de inexistencia de normativa específica y si ésta fuera indispensable, formularán las propuestas pertinentes. Según corresponda, se preservarán las condiciones especiales de tratamiento de datos en sectores específicos.

Dentro de los treinta (30) días hábiles subsiguientes a la emisión de la opinión técnica favorable de la Autoridad Nacional de Protección de Datos Personales, las citadas entidades deberán aprobar o, de ser el caso, impulsar la aprobación de las correspondientes propuestas normativas.

Quinta.- Bancos de datos personales preexistentes

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

Sexta.- Habeas Data

Las normas establecidas en el Código Procesal Constitucional sobre el proceso de Habeas Data se aplican en el ámbito constitucional, independientemente del ámbito administrativo materia de la presente Ley. El procedimiento administrativo establecido en la presente Ley no constituye vía previa para el ejercicio del derecho vía proceso constitucional.

Proyecto de Ley

Sétima.- Competencias del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI

En materia de infracción a los derechos de los consumidores en general mediante los servicios e información brindados por las Centrales Privadas de Información de Riesgos - CEPIRS o similares, en el marco de las relaciones de consumo son aplicables las normas generales sobre protección al consumidor, siendo el ente competente para la supervisión de su cumplimiento la Comisión de Protección al Consumidor del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI, la que deberá velar por la permanencia de la idoneidad de los servicios y por la transparencia de la información que se brinde a los consumidores, sin perjuicio de la competencia de la Autoridad Nacional de Protección de Datos Personales para salvaguardar los derechos de los titulares de la información administrada por las CEPIRS o similares.

Octava.- Información sensible

Para efectos de lo dispuesto en la Ley N° 27489, Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información, se entenderá por información sensible la definida como dato sensible por la presente Ley.

Igualmente, precísese que la información confidencial a que se refiere el numeral 5) del artículo 17° del Texto Único Ordenado de la Ley N° 28706, Ley de Transparencia y Acceso a la Información Pública constituye dato sensible conforme a los alcances de esta Ley.

Novena.- Inafectación de facultades de la Administración Tributaria

Lo dispuesto en la presente Ley no se interpretará en detrimento de las facultades de la Administración Tributaria respecto de la información que obre y requiera para sus registros, así como para el cumplimiento de sus funciones.

Décima.- Financiamiento

La realización de las acciones necesarias para la aplicación de la presente Ley se ejecuta con cargo al presupuesto institucional del pliego Ministerio de Justicia y de los recursos a los que hace referencia el artículo 36° de esta norma, sin demandar recursos adicionales al Tesoro Público.

Décimo primera.- Vigencia

La presente Ley entrará en vigencia en el plazo de treinta (30) días hábiles contado a partir de la publicación de su reglamento en el diario oficial "El Peruano", salvo lo previsto en el Título II, en el primer párrafo del artículo 32° y en la Primera, Segunda, Tercera, Cuarta y Décima Disposiciones Complementarias Finales, las que regirán a partir del día siguiente de la publicación de la presente Ley.

Comuníquese al señor Presidente de la República para su promulgación.

ALAN GARCÍA PÉREZ
Presidente Constitucional de la República

JAVIER VELÁSQUEZ QUESQUÉN
Presidente del Consejo de Ministros

EXPOSICIÓN DE MOTIVOS

1. INTRODUCCION

El fenómeno de la informática se ha convertido en el símbolo emblemático de la cultura contemporánea[1]. Al reducir dramáticamente el costo de generar, almacenar, trasmitir y procesar información en todos los sectores de la economía, la informática ha transformado la manera de concebir la organización y la estructura misma de nuestras sociedades, así como las pautas de comportamiento de las personas.

En suma, la informática ha alterado la realidad económica, social y cultural en la que se basaba la sociedad anterior, haciendo de la información el elemento clave del poder. A la luz de esta nueva realidad, la sociedad actual ha sido denominada como Sociedad de la Información.

Pero si bien es cierto, la información es poder y que sin ella ningún gobierno moderno es capaz de cumplir sus fines, también lo es que el uso indebido o abusivo de la informática puede amenazar de muerte el desarrollo de las instituciones democráticas. Se hace pues, imprescindible someter los avances informáticos a una evaluación crítica sobre sus consecuencias. El progreso de la informática debe propender siempre al desarrollo de la humanidad y, en consecuencia, en ningún caso afectar el pleno ejercicio de los derechos fundamentales. No obstante, la actitud frente a la informática no debe ser defensiva. De lo que se trata es de asegurar el control democrático y el ejercicio social de la informática.

En este contexto, un tema de especial trascendencia está dado por el problema de las relaciones entre información e intimidad[2] que puede derivar en un fenómeno de manipulación y control social inimaginables.

Al respecto, resulta clarificante Pérez Luño cuando comenta que ya en 1972 una sociedad de información comercial de los Estados Unidos había almacenado datos personales sobre 130 millones de personas que, tras su adecuada programación, podían ser transmitidos a sus clientes en más de diez mil aspectos diferentes (por edad, profesión, sexo, ingresos, automóvil o vivienda poseídos, pertenencia a sindicatos, partidos o sociedades mercantiles, culturales o recreativas).[3] O cuando recuerda que la comunidad académica de Estados Unidos sufrió una conmoción al saber que, durante la etapa de contestación estudiantil, diversas universidades que contaban con bibliotecas informatizadas proporcionaron a la policía relaciones exhaustivas de las lecturas de aquellos profesores y/o alumnos sospechosos de ser contestatarios o disidentes[4].

Los bancos de datos lo registran todo: las compañías de viajes conocen el número de veces que hemos viajado al interior y exterior del país, la pizzería sabe qué tipo de

---

[1] García González, Aristeo. La Protección de Datos Personales, Derecho Fundamental del Siglo XXI. Un Estudio Comparado. En Revista de Derecho Informático. No. 100 - Noviembre del 2006. Editor Alfa-Redi. Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=7851

[2] Pérez Luño, Antonio Enrique. Derechos Humanos, Estado de Derecho y Constitución. Tecnos, Madrid, 2003. p. 337.

[3] Ibid. p.348.

[4] Ibid. p. 366.

pizza pedimos, el supermercado sabe qué marca de abarrotes compramos, la compañía de seguros sabe cuántos registros tenemos a las clínicas y por qué conceptos, la farmacia conoce qué medicamentos adquirimos y con qué frecuencia.

Cobra entonces actualidad la peligrosidad de las técnicas over-all computer referidas al cruce de bancos de datos que permite un control exhaustivo de la población, así como la peligrosidad del trazado de un perfil completo de las personas[5]. Huelgan las reflexiones sobre este tema cuando se habla de los delitos informáticos, esto es, de los casos en que de manera ilegal se accede a los datos personales contenidos en bancos de datos[6].

Urge entonces establecer garantías que tutelen la vida privada de las personas frente a la agresión de la informática. Esta exigencia viene encontrando eco en diversas reuniones internacionales, en la legislación de múltiples países - mayoritariamente europeos - y en el desarrollo jurisprudencial de otros. A consecuencia de todo ello aparece la protección de datos personales como una respuesta organizada para el control de la informática.

En la construcción del enfoque de este derecho ha jugado un papel relevante la sentencia del Tribunal Constitucional Federal Alemán del 15 de diciembre de 1983, a propósito de la Ley del Censo de Población del 4 de marzo de 1982, a la que declara parcialmente inconstitucional por no respetar el "derecho a la autodeterminación informativa", entendido como la facultad de determinar quién, qué, cuándo y con qué motivo puede conocer los datos que le conciernan. Esta fue la primera aproximación conceptual al tema a nivel mundial.

Actualmente, en contexto con la Sociedad de la Información, el "derecho a la protección de datos personales" también conocido como "derecho a la autodeterminación informativa" o "libertad informática" entraña dos aspectos complementarios entre sí: uno negativo que se traduce en el derecho a prohibir la difusión de la información de carácter personal[7]; y otro positivo que implica el derecho de controlar los datos concernientes a la propia persona y, en tal sentido, desarrollar una actividad de inspección, verificación o cancelación, asimilable al derecho de rectificación en las informaciones publicadas en los medios de comunicación.[8] Así pues, hoy en día, el derecho fundamental a la protección de los datos personales ha cobrado independencia y autonomía ante el derecho a la intimidad. En efecto, la actitud pasiva de simple defensa de nuestros datos personales – propia del derecho a

---

[5] Ibid. p. 367.

[6] En el documento de Grupo de Trabajo eLAC 2007- Meta 25 eLAC 2007: Regulación en la Sociedad de la Información en América Latina y el Caribe. Propuestas normativas sobre Privacidad y Protección de Datos y Delitos Informáticos y por Medios Electrónicos, p. 60, se definen los delitos informáticos como aquellas conductas ilícitas que afectan el bien jurídico "información en formato digital". Se trata de afectaciones a la confidencialidad, integridad, disponibilidad o uso de la información o de sus sistemas informacionales de soporte.

[7] En 1948, la Declaración Universal de los Derechos Humanos desarrolló el derecho a la intimidad, concibiéndolo como el derecho a no ser objeto de injerencias arbitrarias en la vida privada, la familia, el domicilio o la correspondencia, ni de ataques a la honra o la reputación, y a ser protegido contra ellas. El derecho a la intimidad, así concebido, respondía a un **concepto más bien estático** y fue recogido en la mayoría de los textos constitucionales. Esta concepción se ha quedado de lado. (García González, op. cit. p. 10).

[8] Pérez Luño, op. cit. p. 364.

la intimidad -, pasa a complementarse con una postura activa, con la posibilidad de ejercer el control sobre el caudal de información que puede existir en los diferentes bancos de datos sobre nuestra persona. Y es que el peligro para la privacidad de la persona no radica en la acumulación de información sobre ella, sino en la pérdida de la capacidad de disposición de tal información y de determinar a quién y con qué objeto se transmite.

2. SITUACIÓN INTERNACIONAL

La discusión teórica y los primeros textos normativos encaminados a regular los aspectos más acuciantes de la tensión entre la informática y los derechos fundamentales aparecieron en los países europeos donde, junto a un mayor desarrollo tecnológico, se daba también una mayor sensibilidad hacia la defensa de tales derechos.

Así, con leyes específicas al respecto, inicialmente destacan Alemania, en 1970, con la Ley Hesse que tuvo por acierto crear la figura del comisario para la protección de la información; Estados Unidos en 1974 con la reconocida Privacy Act, luego sustituida por la Privacy Protection Act de 1980; Nueva Zelanda en 1976 y Canadá en 1977 en el seno de la Commonwealth Británica; así como Francia, Noruega, Dinamarca y Austria que en 1978 dictaron sus propias normas sobre utilización de la informática.

A nivel constitucional son mencionables la Constitución portuguesa de 1976 y la Constitución española de 1978. Sobre el caso español y ya en años más recientes, cabe citar la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), posteriormente sustituida por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPRODA).

Pero la exigencia de tutelar la vida privada de las personas frente a la informática rebasó desde el principio la esfera estricta del derecho interno para plantearse como una exigencia del orden jurídico internacional.

Ciertamente, ya en 1968 la Asamblea General de las Naciones Unidas había adoptado una Resolución sobre los derechos del hombre y los progresos de la ciencia y la técnica. En 1971, informes y estudios comparados sobre la materia habían sido presentados a iniciativa de las Naciones Unidas y de la UNESCO. Y en 1973 el Comité de Ministros del Consejo de Europa había aprobado una Resolución sobre la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado, a la que siguió en 1974 la Resolución sobre los bancos de datos en el sector público, primeros textos internacionales relativos a la protección de datos personales.

Hasta la fecha, diversos textos internacionales se han elaborado en Europa, siendo uno de los más importantes el "Convenio 108 del 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales", norma supranacional que resulta ampliada y actualizada por la Directiva Nº 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", la que constituye, quizás, el modelo mejor logrado de regulación en esta materia, ya que en ella encuentran desarrollo la mayor cantidad de aspectos expresivos del régimen, incluyendo la cuestión propiamente internacional referida al flujo de datos transfronterizos. No podemos dejar de señalar que a través de la Carta de los

Derechos Fundamentales de la Unión Europea de 2000 (2000/C 364/01)[9] se consagra la tutela al derecho de protección de datos de carácter personal[10]. Tampoco podemos dejar de referirnos a regulación incluso más específica sobre el tema y es la Directiva 2002/58/CE de Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Múltiples han sido, por otra parte, los foros mundiales de discusión que vienen ocupándose del tema informático. Por la brevedad a que debe restringirse este documento, citemos entre los más recientes la primera y segunda fases de la Cumbre Mundial sobre la Sociedad de la Información, celebradas en Ginebra en diciembre de 2003 y en Túnez en noviembre de 2005, con el fin de encausar el potencial de las tecnologías de la información y de las comunicaciones para promover los objetivos de desarrollo del Milenio; igualmente, la Organización para la Cooperación y el Desarrollo Económico (OCDE)[11], que mediante lineamientos sobre protección de la privacidad y flujos transfronterizos de datos personales, busca prevenir potenciales limitaciones al flujo de información que podrían afectar el desarrollo económico.[12]

Resulta importante también señalar que en el 2009, bajo la coordinación de la Agencia Española de Protección de Datos, los garantes de la privacidad de casi cincuenta países, desarrollaron el documento denominado "Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad, en relación con el Tratamiento de Datos de Carácter Personal", acogido favorablemente por la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre del citado año, en la ciudad de Madrid. En este documento se plasman los múltiples enfoques que admite la protección de este derecho, integrando legislaciones de los cinco continentes.

En contexto con la globalización, la protección de datos personales es hoy en día también parte de la agenda de los países latinoamericanos y en ello merece

---

[9] La Carta de los Derechos Fundamentales de la Unión Europea fue firmada y proclamada el 7 de diciembre de 2000 con ocasión del Consejo Europeo de Niza, por los Presidentes del Parlamento Europeo, del Consejo y de la Comisión y recoge en un único texto, por primera vez en la historia de la Unión Europea, el conjunto de los derechos civiles, políticos, económicos y sociales de los ciudadanos europeos y de todas las personas que viven en el territorio de la Unión.

[10] "Artículo 8º: Protección de datos de carácter personal
1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas queda sujeto al control de una autoridad independiente."

[11] La OCDE es una organización de cooperación internacional, cuyo objetivo es coordinar las políticas económicas y sociales de los Estados que la conforman. Fue fundada en 1961 y su sede central se encuentra en la ciudad de París, Francia. Los países miembros actualmente son Alemania, Austria, Bélgica, Canadá, Dinamarca, España, Estados Unidos, Francia, Gracia, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido, Suecia, Suiza, Turquía, Japón, Finlandia, Australia, Nueva Zelanda, México, República Checa, Corea del Sur, Hungría, Polonia y Eslovaquia.

[12] En el 2007, la OCDE propició que los países miembros renovaran los compromisos de cooperación mutua con miras a promover el mejoramiento de los marcos legales domésticos para facilitar la cooperación y el desarrollo de mecanismos internacionales de supervisión y control, a fin de garantizar el cumplimiento de las leyes de protección de datos personales.

destacarse el rol relevante de diversos foros y organizaciones de cooperación internacional que han venido trabajando por el reconocimiento del derecho a la protección de datos personales y el desarrollo de principios de armonización normativa.

Conviene mencionar, por ejemplo, la Declaración de Santa Cruz de la Sierra, suscrita el 2003, con motivo de la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, por la que se reconoce la protección de datos personales como derecho fundamental de las personas y se destaca la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos, según alcances de la Declaración de La Antigua[13]; la aprobación del "Marco sobre Privacidad de APEC"[14], en Chile, el 2004, por los ministros de los países miembros de este Foro – entre ellos, el Perú por cierto -, por el que se desarrollan los principios comunes a la protección de datos personales, con miras a favorecer el flujo de información en la Región Asia – Pacífico; del mismo modo, la posterior creación del Grupo Permanente de Trabajo de Comercio Electrónico del APEC; además, el Compromiso de Río de Janeiro y el Plan de Acción de la Sociedad de la Información de América Latina y el Caribe (eLAC 2007), aprobados en Brasil el 2005, en el marco de la Conferencia Regional Ministerial de América Latina y el Caribe Preparatoria para la Segunda Fase de la Cumbre Mundial de la Sociedad de la Información y en los que se definen una agenda, un plan de acción y una plataforma para impulsar la cooperación regional en materia de tecnologías de la información y de las comunicaciones; la Red Iberoamericana de Protección de Datos promovida desde la Comunidad Europea, que ha logrado incluir en diversas declaraciones políticas de países de Iberoamérica la necesidad de adoptar lineamientos en materia de protección de datos; de la misma manera, el Monitor de Privacidad y Acceso a la Información en América Latina y el Caribe promovido por la UNESCO, que en el 2006 realizara un taller en Lima, sobre temas de cooperación y propusiera mecanismos de armonización normativa en la materia; finalmente y más recientemente, el Compromiso de San Salvador, el 2008, adoptado en la II Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe, por el que se aprueba el Plan de Acción sobre la Sociedad de la Información de América Latina y el Caribe (eLAC 2010) y se adopta el Mecanismo Regional para su Seguimiento.

Varios son los países que en Sudamérica reconocen el derecho a la protección de datos personales al interior de sus Constituciones Políticas. Tal es el caso de Brasil en 1988, Colombia en 1991, Paraguay en 1992, Perú en 1993 y Argentina en 1994.

Continuando con Sudamérica, entre las leyes expedidas al momento, cabe mencionar por lo pronto a Argentina, a través de la Ley Nº 25326 del 04.10.2000, posteriormente reglamentada por el Decreto Nº 1558/2001 del 29.11.2001; Chile con la Ley Nº 19.628 del 28.08.1999; Paraguay, con la Ley Nº 1682/2001 del 28.12.2000; Uruguay, con la Ley Nº 18.331 del 11.08.2008. En Norteamérica, el caso más reciente con legislación en materia de protección de datos personales está en el Distrito Federal de Méjico, con la Ley del 06.11.2008.

---

[13] La Declaración de la Antigua se emitió con motivo de la celebración del Seminario sobre Protección de Datos Personales en Iberoamérica - II Encuentro Latinoamericano de Datos Personales, impulsado por la Agencia Española de Protección de Datos, con el apoyo de la Agencia Española de Cooperación Internacional (AECI) y la Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP), celebrado en La Antigua (Guatemala), los días 2 a 6 de junio de 2003.

[14] Conocido según texto original como "APEC Privacy Framework".

3. SITUACIÓN NACIONAL

En orden al derecho internacional, debemos tener presente que son normas jurídicas para nuestro país el artículo 12° de la Declaración Universal de los Derechos del Hombre, el artículo 17° del Pacto Internacional de Derechos Civiles y Políticos, el artículo 5° de la Declaración Americana de los Derechos y Deberes del Hombre de 1948 y el artículo 11° del Pacto de San José de Costa Rica. En términos parecidos, todas estas normas consagran la protección de la honra, reputación, y la vida privada y familiar, prohibiendo injerencias arbitrarias que bien pueden derivar del uso de la informática.

Respecto del derecho nacional, nuestra Constitución Política de 1993 reconoce el instituto de la protección de datos personales como el derecho fundamental de toda persona a que los servicios informáticos[15], computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar[16]. En el mismo texto constitucional se dispone su tutela a través del habeas data como acción de garantía constitucional contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que lo vulnere o amenace[17].

Mediante sentencia emitida 5 años después, en 1998, nuestro Tribunal Constitucional ha sostenido que la protección a este derecho a través del habeas data comprende acceder a los registros de información almacenados en centros informáticos o computarizados, cualquiera sea su naturaleza a fin de rectificar, actualizar y excluir determinado conjunto de datos personales, o impedir se propague información que pueda ser lesiva al derecho constitucional a la intimidad.[18] Posteriormente, también 5 años después, mostrando su preocupación al respecto, y reiterándose y ampliando lo anterior, nuestro Tribunal Constitucional ha señalado que la protección a este derecho - al que denominó "autodeterminación informativa" conforme a la denominación que le asigna parte de la doctrina – a través del habeas data comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información, así como la (o las) persona(s) que recabaron dicha información. En segundo lugar, el hábeas data puede tener la finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro

---

[15] La referencia a los servicios informáticos alude a los bancos de datos. (García Toma, Víctor. Análisis Sistemático de la Constitución Peruana de 1993. Tomo I. Fondo de Desarrollo Editorial, 1998. p. 84).

[16] Constitución Política del Perú, artículo 2, inciso 6.

[17] Constitución Política del Perú, artículo 200, inciso 3.

[18] Sentencia del Tribunal Constitucional de fecha 08.07.1998 recaída en el Expediente Nº 666-96-HD/TC. Disponible en: http://www.tc.gob.pe/jurisprudencia/1998/00666-1996-HD.html

o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados[19].

En el 2004, el Código Procesal Constitucional, ocupándose del habeas data y siguiendo la línea desarrollada por el Tribunal Constitucional, estableció que se puede acudir a este proceso para conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a la 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, para hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales. Agrega que tratándose de la protección de datos personales, podrán acumularse las pretensiones de acceder y conocer informaciones de una persona, con las de actualizar, rectificar, incluir, suprimir o impedir que se suministren datos o informaciones[20].

Cabe referirnos también al Código Penal de 1991, aprobado años antes del reconocimiento constitucional del derecho fundamental a la protección de datos personales, en el que se plantea como tipo penal el uso indebido de archivos computarizados, estableciéndose que comete delito el que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas[21]. Más tarde, en el 2000 se incorporan al Código Penal los denominados delitos informáticos, configurándose como delito el ingreso indebido a una base de datos para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar la información en tránsito o que ella contenga[22] (delito conocido en la doctrina como espionaje informático o intrusismo).

Resulta pertinente también citar la Ley de Transparencia y Acceso a la Información Pública[23], que se ocupa de regular los casos de acceso a la información pública a cargo de la Administración Pública, en desarrollo del derecho fundamental al acceso a la información[24]. A tenor de dicha ley, bien se advierte que en la práctica el ejercicio de este derecho puede muchas veces entrar en conflicto con el derecho a la protección de datos personales, cuando aquéllos son de carácter confidencial[25], de ahí la importancia de su adecuada regulación.

---

[19] Sentencia del Tribunal Constitucional de fecha 29.01.2003 recaída en el Expediente Nº 1797-2002-HD/TC. Disponible en: http://tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html

[20] Código Procesal Constitucional, artículos 61, 62 y 64.

[21] Código Penal, Capítulo II: Violación de la Intimidad, artículo 157.- Uso indebido de archivos computarizados.

[22] Código Penal, Capítulo X: Delitos Informáticos, artículo 207-A.- Delito Informático. Artículo incorporado mediante Ley Nº 27309 del 17.07.2000.

[23] Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública, cuyo Texto Único Ordenado ha sido aprobado por Decreto Supremo Nº 043-2003-PCM.

[24] Artículo 2º, inciso 5 de la Constitución Política. "Toda persona tiene derecho:
(...)
5) A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.
(...)."

En relación con las leyes dictadas sobre aspectos propios a la regulación de los datos personales, se encuentran vigentes la Ley N° 27489 que regula las centrales privadas de información de riesgos y de protección al titular de la información, que es propiamente la Ley sobre bancos de datos de solvencia patrimonial y de crédito; la Ley N° 28493 que regula el uso del correo electrónico comercial no solicitado (SPAM) y su Reglamento aprobado por Decreto Supremo N° 031-2005-MTC, así como el Texto Único Ordenado de la Ley de Protección al Consumidor aprobado por Decreto Supremo N° 006-2009-PCM, por cuyo Anexo – 5ª Disposición se regulan los sistemas de promociones a distancia.

Pero este marco jurídico no es suficiente pues sólo garantiza la protección de datos personales en determinados sectores, y quizá no sea precisamente el más adecuado. En tal sentido, con el propósito de clarificar el ámbito de extensión del derecho a la protección de datos personales, delimitar con toda precisión sus alcances, reforzar su defensa y avanzar hacia la plena eficacia en su ejercicio, hace falta aun una ley singular sobre la protección de datos personales que en lo posible observe los avances científicos y tecnológicos actuales. Nuestros gobernantes y autoridades en general así lo han reconocido y a ello se han comprometido.

Por otro lado, la dación de un marco regulatorio específico en materia de protección de datos personales constituiría un importante avance para el cumplimiento de uno de los compromisos asumidos por el Estado peruano a través de la Vigésimo Novena Política de Estado del Acuerdo Nacional denominada "Acceso a la información, Libertad de Expresión y Prensa"[26]; constituye una potestad del Perú como Estado Parte en el Tratado de Libre Comercio celebrado con los Estados Unidos[27], mientras que en el

---

[25] Artículo 17° inciso 5), sobre excepciones al ejercicio del derecho: Información confidencial. El derecho de acceso a la información pública no podrá ser ejercido respecto de lo siguiente:
(...)
5. La información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal. En este caso, sólo el juez puede ordenar la publicación sin perjuicio de lo establecido en el inciso 5 del artículo 2 de la Constitución Política del Estado.

[26] *Vigésimo Novena Política de Estado del Acuerdo Nacional*
Acceso a la Información, Libertad de Expresión y Libertad de Prensa
"(...)
Con el objetivo de garantizar el acceso a la información y la libertad de expresión, el Estado: (...) (e) procurará el equilibrio entre el **derecho a la protección de la intimidad personal y la seguridad nacional, con el derecho al libre acceso de la información del Estado y a la libertad de expresión**; (...)" (Lo resaltado es nuestro)
Disponible en: http://www.acuerdonacional.gob.pe/DocumentosAN/2008/castellano.pdf

[27] Cabe transcribir al respecto los numerales 3 y 4 del artículo 14.2 ° Acceso y Uso de los Servicios Públicos de Telecomunicaciones del Capítulo 14°, Telecomunicaciones, del Tratado de Libre Comercio con Estados Unidos, vigente en nuestro país a partir del 1 de febrero de 2009:
"(...)
3. Cada Parte garantizará que las empresas de otra Parte puedan usar servicios públicos de telecomunicaciones para mover información en su territorio o a través de sus fronteras y para tener acceso a la información contenida en bancos de datos o almacenada de forma que sea legible por una máquina en el territorio de cualquiera de las Partes.
4. No obstante lo dispuesto en el numeral 3, una Parte podrá tomar medidas que sean necesarias para:
(a) garantizar la seguridad y confidencialidad de los mensajes; o
(b) **proteger la privacidad de datos personales no públicos de los suscriptores de servicios públicos de telecomunicaciones**, siendo entendido que tales medidas no se apliquen de tal manera que pudieran constituir un medio de discriminación arbitraria o injustificable, o alguna restricción encubierta al comercio de servicios." (Lo resaltado es nuestro)

marco del Tratado de Libre Comercio suscrito con Canadá[28] constituye un compromiso de mejores esfuerzos. Más aun, constituye también un compromiso asumido en el marco del Plan de Acción del eLAC 2007 a través de su meta 25[29] y actualmente del Plan de Acción del eLAC 2010 a través de su meta 78[30]; además, respondería a la estrategia 3.3 del objetivo 3[31] del Plan de Desarrollo de la Sociedad de la Información en el Perú – la Agenda Digital[32].

Sin embargo, el propósito que nos debe convocar no debe ser sólo definir una legislación básica para la tutela del derecho fundamental a la protección de datos personales, sino una legislación que permita el desarrollo regional, transfronterizo, en un marco internacional, a partir del aseguramiento de la libre circulación de datos personales. Insertos en un mundo globalizado y con el objeto de afrontar los desafíos que se presentan, esta no es sólo una opción, sino el único camino viable y este es el empeño de este proyecto de Ley.

---

[28] El Tratado de Libre Comercio entre el Perú y Canadá, vigente en nuestro país a partir del 1 de agosto de 2009, establece en el Capítulo 15 (Comercio Electrónico) lo siguiente:
"Artículo 1507: Protección de la Información Personal
1. Las Partes reconocen la importancia de proteger la información personal en el ambiente en línea.
2. Con este fin, **cada Parte debería**:
(a) **Adoptar o mantener medidas legales, reglamentarias y administrativas para la protección de la información personal de los usuarios que participen en el comercio electrónico**; y
(b) Intercambiar información y experiencia sobre sus regímenes domésticos de protección de la información personal". (Lo resaltado es nuestro)

[29] Meta 25 del Plan de Acción del eLac 2007, bajo el rubro "Instrumentos de Política" – "Marco Legislativo": 25 Establecer grupos de trabajo subregionales para promover y fomentar políticas de armonización de normas y estándares, con el fin de crear marcos legislativos que brinden confianza y seguridad, tanto a nivel nacional como a nivel regional, **prestando especial atención a la legislación sobre la protección de la privacidad y datos personales**, delitos informáticos y delitos por medio de las TIC, spam, firma electrónica o digital y contratos electrónicos, como marco para el desarrollo de la sociedad de la información. Plazo: noviembre de 2005. (Lo resaltado es nuestro).
Disponible en:
http://www.eclac.org/socinfo/noticias/noticias/2/32362/2008-1-TICs-Compromiso_de_San_Salvador.pdf

[30] Meta 78 del Plan de Acción del eLac 2010, bajo el Capítulo VI: Instrumentos de política y estrategias: **Renovar el mandato del grupo de trabajo en materia del marco legal de la sociedad de la información** para facilitar el diálogo y la coordinación de las diversas iniciativas regulatorias a nivel regional y local que pudieran favorecer la armonización normativa de la región. (Lo resaltado es nuestro).
Disponible en:
http://www.eclac.org/socinfo/noticias/noticias/2/32362/2008-1-TICs-Compromiso_de_San_Salvador.pdf

[31] Objetivo 3 del Plan de Desarrollo de la Sociedad de la Información en el Perú – la Agenda Digital: Desarrollar el sector social del Perú garantizando el acceso a servicios sociales de calidad, promoviendo nuevas formas de trabajo digno, incentivando la investigación científica e innovación tecnológica, así como asegurando la inclusión social y el ejercicio pleno de la ciudadanía. Estrategia 3.3 Contribuir al ejercicio amplio y pleno de la democracia y la garantía del Estado de Derecho con la aplicación de las TICs. Acción 3.3.1 **Establecimiento de normas que faciliten el derecho de la ciudadanía a la información, a la comunicación y al resguardo de datos confidenciales.** (Lo resaltado es nuestro)
Disponible en: http://www.codesi.gob.pe/codesi/downloads/MATRIZ_DEL_PLAN_200606.pdf

[32] El Plan de Desarrollo de la Sociedad de la Información en el Perú – la Agenda Digital ha sido aprobado por Decreto Supremo Nº 031-2006-PCM del 21 de junio de 2006 y constituye un documento de política que contiene las acciones, estrategias, metas, y políticas específicas necesarias para el adecuado desarrollo, implementación y promoción de la Sociedad de la Información en el Perú, a fin de alcanzar la modernización del Estado y desarrollar un esquema real y coherente en beneficio de la población en general. Para su implementación, seguimiento y monitoreo se cuenta con una Comisión Multisectorial de carácter permanente, presidida por el Presidente del Consejo de Ministros e integrada por los Ministros de Transportes y Comunicaciones, Producción y Educación. Esta comisión se denomina Comisión Multisectorial para el Desarrollo de la Sociedad de la Información (CODESI).

4. PROYECTO DE LEY

El texto del proyecto de Ley se encuentra integrado por cuarenta artículos distribuidos en ocho Títulos, así como por once Disposiciones Complementarias Finales.

En su estructura normativa puede distinguirse una parte general dedicada a la proclamación del derecho a la protección de datos personales y sus manifestaciones, integrada por los Títulos I al V; y, una parte especial, en la que se establecen los mecanismos organizativos e institucionales para el adecuado funcionamiento de los bancos de datos personales, formada por los Títulos VI al VIII.

Hecha esta presentación del esquema del proyecto y conforme al mandato contenido en el Reglamento de la Ley Marco para la Producción y Sistematización Legislativa aprobado por Decreto Supremo Nº 008-2006-JUS, pasamos a explicar los aspectos más relevantes que contiene.

- Título I: Disposiciones Generales.

En este Título se formulan las disposiciones generales del proyecto de ley, referidas a su objeto, definiciones y ámbito de aplicación.

El derecho a la protección de datos personales es un derecho fundamental de tercera generación[33] estrechamente vinculado a otros derechos de la misma naturaleza, pero de primera generación, como son el derecho al honor, buena reputación, intimidad, voz e imagen propias. Sin duda, por ser además un derecho relacional, su tratamiento inadecuado puede afectar el ejercicio de otros derechos fundamentales, pero particularmente el ejercicio de los mencionados. De ahí que el proyecto de ley no restrinja su objeto a garantizar sólo su adecuado tratamiento, sino que además se preocupe por explicitar que este tratamiento debe efectuarse en un marco de respeto de los derechos fundamentales, en particular el derecho al honor, buena reputación, intimidad, voz e imagen propias.

La definición de datos personales se extiende a toda información sobre una persona natural que la identifica o la hace identificable, por tanto, se ocupa tanto de los datos que afectan la privacidad, como de aquéllos que afectan un ámbito más restringido: la intimidad[34]. Es en este último supuesto que se regulan de manera específica los datos sensibles.

De acuerdo con el proyecto, tienen la naturaleza de datos sensibles los datos personales constituidos por los datos biométricos[35] [36] [37], los datos referidos al origen

---

[33] Los derechos de tercera generación se presentan como una respuesta al fenómeno de la denominada "contaminación de las libertades", término con el que en algunos sectores de la teoría social anglosajona se hace alusión a la erosión y degradación que aqueja a los derechos. (García González, op.cit. p. 4.) Efectuamos esta distinción sólo por efectos académicos, sin conllevar a ninguna priorización de unos frente a otros.

[34] "(...) el derecho a la protección de datos "reconoce a la persona un poder de control sobre la información personal que le concierne, sobre su utilización y destino, para evitar utilizaciones ilícitas, por lo que su protección no sólo se limita a datos íntimos, sino a cualquier información personal, sea o no íntima, siempre que su tratamiento pueda afectar a derechos y libertades de la persona" (García González, op. cit. pág. 25, citando a Herrán Ortiz).

[35] Los datos biométricos revelan rasgos característicos y distintivos de partes físicas o biológicas de la persona que la hacen diferente a cada uno de los otros. En sentido general, la recopilación se lleva a cabo

racial y étnico; las opiniones o convicciones políticas, religiosas, filosóficas o morales; los hábitos personales; la afiliación sindical; y la información relacionada a la salud o a la vida sexual. Privilegiando la seguridad jurídica, se ha optado pues por hacer una enumeración taxativa de éstos. Otras legislaciones, optan más bien por una enumeración abierta. Se precisa que los datos sensibles son objeto de especial protección dado que los riesgos de vulneración de los derechos fundamentales se hace más evidente en el caso de manipulación de esta categoría de dato.

En cuanto al ámbito subjetivo de tutela del proyecto, éste se ha circunscrito a las personas naturales. No ha considerado, en consecuencia, a las personas jurídicas[38]. Esto se debe a la decisión de asumir, más bien, una posición conservadora, basados en que la primera alternativa es la que cuenta con mayor número de precedentes en el derecho comparado de la protección de datos personales, pues esta legislación fue pensada inicialmente para proteger la intimidad de las personas naturales.

Con relación al ámbito objetivo del proyecto, éste se ha extendido tanto a los datos personales ya contenidos en bancos de datos personales, como a los destinados a ser contenidos en ellos, siempre que su tratamiento se realice en el territorio nacional. Al efecto, es importante tener presente que el banco de datos personales es definido por la doctrina como centro de ordenación encargado de acopiar y seleccionar antecedentes de cualquier naturaleza[39] o también como archivo estructurado según criterios específicos relativos a las personas[40]. El proyecto de ley incluye una definición técnica al respecto. Es importante tener en cuenta esta definición a efectos de deslindar adecuadamente los supuestos en que se arremete por ejemplo contra el derecho al honor, buena reputación, intimidad, voz e imagen propias, frente a los supuestos en que se agrede el derecho a la protección de los datos personales, pues según ello corresponderá iniciar una acción de amparo o de habeas data.

---

a través del escaneo de la muestra física (total o parcial) o biológica por un dispositivo biométrico de captación adecuado. La muestra captada es procesada por un software o programa informático o por métodos convencionales y manuales.

[36] Entre otros datos biométricos, cabe citar las huellas digitales, la geometría de la mano, análisis del iris o de la retina, reconocimiento facial o del diafragma, análisis del ADN, lectura del patrón de la voz, datos de imagen (las fotografías son los soportes de datos de imagen por excelencia) inclusive los capturados a través de sistemas de cámaras o de videocámaras o de escáneres corporales, y los datos genéticos. El artículo 8.1 de la Directiva 46/95 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" prohíbe el tratamiento de este tipo de datos considerados "sensibles" por las informaciones que revelan. En lo que respecta a los datos genéticos, éstos también son considerados como datos de la salud.

[37] Recordemos que el 28 de noviembre del 2008, mediante Resolución Administrativa Nº 270-2008-CE-PJ se aprobó la Directiva **"Registro y Control Biométrico de Procesados y Sentenciados Libres"**, la misma que permite garantizar y verificar la identidad de los procesados o sentenciados que se encuentren en libertad, verificando su concurrencia al juzgado en los plazos señalados, de acuerdo a las medidas coercitivas que se le hayan impuesto. (Lo resaltado es nuestro)

[38] A manera de ejemplo, tanto la ley argentina como la ley uruguaya para la protección de datos personales extienden su ámbito de aplicación subjetivo a las personas jurídicas.

[39] García Toma, op. cit. p. 84.

[40] Definición incluida en el Considerando Nº 15 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos".

Se ha excluido del ámbito de aplicación del proyecto no sólo los datos contenidos en bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar, sino también aquéllos contenidos o destinados a ser contenidos en bancos de datos de administración pública cuyo tratamiento resulte necesario para el cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas para la defensa nacional, seguridad pública y sus actividades en materia penal para la investigación y represión del delito.

Cabe mencionar que la protección que se confiere a los datos personales a través del proyecto se extiende tanto a aquéllos objeto de tratamiento por sistemas automatizados, como por sistemas manuales[41].

- Título II: Principios rectores

Los principios son normas que tienen la estructura de mandatos de optimización. Estas normas no determinan exactamente lo que debe hacerse, sino que ordenan "que algo sea realizado en la mayor medida posible, dentro de las posibilidades jurídicas y reales existentes"[42]

Así, el desarrollo de lo que hemos denominado como "principios rectores" es fundamental en la medida que éstos orientan y determinan el comportamiento de todos los que van a participar en el tratamiento de datos personales, señalando las reglas de conducta que ellos deben observar.

Hecha esta breve introducción, en este título se desarrollan ocho principios rectores. Se trata de los principios rectores de legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, disposición de recurso y nivel de protección adecuado.

Los principios consagrados en este título toman su base de los principios propuestos por las Directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales (1980), los Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales de la Organización de las Naciones Unidas (1990), el Marco sobre Privacidad de APEC (2004), el Plan de Acción de la Sociedad de la Información de América Latina y el Caribe (eLAC 2007) aprobado en el marco de la Conferencia Regional Ministerial de América Latina y el Caribe Preparatoria para la Segunda Fase de la Cumbre Mundial de la Sociedad de la Información (2005), y los Estándares Internacionales sobre Protección de Datos Personales y Privacidad, "Resolución de Madrid" (2009).

- Título III: Tratamiento de Datos Personales

En este Título se desarrollan los alcances a que se sujeta el tratamiento de los datos personales, los supuestos en que no se requerirá el consentimiento del titular de datos

---

[41] Esta opción es también la recogida en el artículo 2, Definiciones, literal b) tratamiento, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos".

[42] Bernal Pulido, Carlos. El Derecho de los Derechos. Panamericana, Colombia, 2005. p. 97.

personales para fines de su tratamiento, así como el flujo transfronterizo de datos, también reconocido en otros ámbitos como TID "Transferencia Internacional de Datos".

Para continuar desarrollando los alcances de este Título, resulta indispensable detenernos en el concepto "contenido esencial" y en la reserva de ley para la imposición de limitaciones a los derechos fundamentales. Al respecto, nuestro Tribunal Constitucional explica lo siguiente: "Todo ámbito constitucionalmente protegido de un derecho fundamental se reconduce en mayor o menor grado a su contenido esencial, pues todo límite al derecho fundamental sólo resulta válido en la medida de que el contenido esencial se mantenga incólume"[43]. Y luego, "El contenido esencial de un derecho fundamental está constituido por aquel núcleo mínimo e irreductible que posee todo derecho subjetivo reconocido en la Constitución, que es indisponible para el legislador, debido a que su afectación supondría que el derecho pierda su naturaleza e identidad. En tal sentido, se desatiende o desprotege el contenido esencial de un derecho fundamental, cuando este queda sometido a limitaciones que lo hacen impracticable y lo despojan de la protección constitucional otorgada."[44] Es así que (los derechos fundamentales) pueden ser restringidos o limitados mediante ley[45]. El respeto que debe el legislador al contenido esencial para establecer cualquier limitación a un derecho fundamental ha sido también previsto en la doctrina, jurisprudencia y en legislación extranjeras e incluso en la supranacional europea[46]. El respeto al contenido esencial, sin embargo, no ha impedido la incorporación de limitaciones y es que "ningún derecho fundamental puede entenderse ilimitado en su ejercicio"[47].

Acorde con lo anterior y tal y como ocurre en otros países[48], en el proyecto de Ley se ha establecido que sólo el legislador podrá limitar el ejercicio del derecho fundamental a la protección de datos personales y que tales limitaciones deberán respetar su contenido esencial. El contenido esencial de los derechos fundamentales no puede determinarse a priori, sino sólo en cada caso concreto, así ha sido establecido por nuestro Tribunal Constitucional.[49] En todo caso, como veremos a continuación, los

---

[43] Tribunal Constitucional del Perú, La Constitución en la Jurisprudencia del Tribunal Constitucional. Gaceta Jurídica, 2006, p.23, L 012, expediente Nº 1417-2005-AA, 08/07/05, P. FJ. 21.

[44] Tribunal Constitucional del Perú, op. cit., p.24, L 014, expediente Nº 1042-2202-AA, 06/12/02, S2, FJ. 2.2.4.

[45] Expediente Nº 9038-2005-PHC/TC, 28.11.200, FJ 4, que se remite al expediente N° 51091-2002-HC/TC.

[46] En efecto, el artículo 52º de la Carta de los Derechos Fundamentales de la Unión Europea, establece lo siguiente:
"Artículo 52º
Alcance de los derechos garantizados
1. Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el **contenido esencial** de dichos derechos y libertades. (...)"
(Lo resaltado es nuestro)

[47] En: Tribunal Constitucional del Perú. op. cit., p. 29, L035, Expediente Nº 2663-02003-HC, 23/03/04, P, FJ.6.

[48] La Ley Fundamental de Bonn de 1949 y la Constitución española de 1978 contienen cláusulas en virtud a las cuales se establece que en la limitación de los derechos el legislador deberá respetar su contenido esencial. Así consta en el Expediente Nº 2868-2004-AA, 24/11/04, S2, FJ.16. del Tribunal Constitucional. (Tribunal Constitucional del Perú, op. cit., p.30, L 039).

[49] Expediente N° 1417- 2005-AA, 08/07/2005, FJ. 21. "Este Tribunal Constitucional considera que la determinación del contenido esencial de los derechos fundamentales no puede efectuarse *a priori,* es

límites que se impongan deben fundamentarse en la necesidad de proteger o preservar otros bienes, valores o derechos constitucionales.

En el proyecto de Ley se regulan limitaciones al derecho fundamental a la protección de datos personales, que inciden en la no necesidad de consentimiento para su tratamiento constatados ciertos supuestos[50]. Para la determinación de estos supuestos se ha tenido en cuenta el criterio impuesto hace años ya por nuestro Tribunal Constitucional: "Los límites que pueden establecerse por el ejercicio de estos derechos (fundamentales) son varios y, como regla general, se determinan tomando en consideración la naturaleza de los derechos en cuestión. No obstante, en determinados supuestos, el legislador puede fijar una diversa clase de límites a tales libertades, límites cuya justificación se encuentra en las relaciones especiales de sujeción bajo las que se encuentran determinados individuos (respecto a la administración pública).[51] En la medida en que los límites especiales derivados de una relación de sujeción especial tienen por propósito garantizar la efectividad de los intereses públicos a los que sirve una dependencia pública, los alcances de esta limitación deben entenderse concretamente referidos a los intereses públicos cuya efectividad se persigue asegurar con la limitación de los derechos constitucionales[52] Y es que, como señala Bernal Pulido, las restricciones (o limitaciones) que se apliquen a los derechos fundamentales deben ser razonables y proporcionadas, esto es, deben estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos.[53] [54] Así ha quedado establecido también en el proyecto de ley.

---

decir, al margen de los principios, los valores y los demás derechos fundamentales que la Constitución reconoce. En efecto, en tanto el contenido esencial de un derecho fundamental es la concreción de las esenciales manifestaciones de los principios y valores que lo informan, su determinación requiere un análisis sistemático de este conjunto de bienes constitucionales, en el que adquiere participación medular el principio-derecho de dignidad humana, al que se reconducen, en última instancia, todos los derechos fundamentales de la persona." Asimismo, FJ. 22. "Si bien es cierto que la exactitud de aquello que constituye o no el contenido protegido por parte de un derecho fundamental, y, más específicamente, el contenido esencial de dicho derecho, sólo puede ser determinado a la luz de cada caso concreto, no menos cierto es que existen determinadas premisas generales que pueden coadyuvar en su ubicación. Para ello, es preciso tener presente la estructura de todo derecho fundamental."

[50] El consentimiento, tal y como se señala en el proyecto de ley, es requisito para cualquier tratamiento de datos personales y consiste en la manifestación de voluntad previa, informada, expresa e inequívoca de su titular. En el caso de datos sensibles, el consentimiento además debe constar por escrito.

[51] Tribunal Constitucional del Perú, op. cit., p.33, L 051, expediente Nº 0866-2000-AA, 10/07/02, P, FJ.3.

[52] Tribunal Constitucional del Perú, op. cit., p.34, L 051, expediente Nº 0866-2000-AA, 10/07/02, P, FJ. 4.

[53] Bernal Pulido, op. cit., p. 253.

[54] En el mismo sentido: "(...) Los límites (a los derechos fundamentales) pueden ser intrínsecos o extrínsecos (...)" y, refiriéndose a los segundos, que son los que nos ocupan, define éstos como"(...) aquellos que se deducen del ordenamiento jurídico, cuyo fundamento se encuentra en la necesidad de proteger o preservar otros bienes, valores o derechos constitucionales (...)".En: Tribunal Constitucional del Perú. op. cit., p. 29, L035, Expediente Nº 2663-02003-HC, 23/03/04, P, FJ.6.

Igualmente, cabe remitirnos al artículo 52º de la Carta de los Derechos Fundamentales de la Unión Europea, parte final, que señala que sólo se podrán introducir limitaciones a los derechos fundamentales, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

- Título IV: Derechos del titular de datos personales

Los principios rectores de protección de los datos personales tienen su expresión en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento.

Acorde con lo anterior, tales derechos se desglosan en derecho de información, acceso, actualización, inclusión, rectificación y supresión, a impedir el suministro[55], oposición al tratamiento[56] y al tratamiento objetivo de sus datos personales[57]. Asimismo, se establece el derecho a la tutela que puede ejerce a través de la vía administrativa mediante la reclamación ante la Autoridad Nacional de Protección de Datos Personales o, alternativamente, en la vía jurisdiccional mediante la acción constitucional correspondiente ante el Poder Judicial[58]; finalmente, el derecho a ser indemnizado por el daño sufrido como consecuencia de la contravención a las disposiciones del proyecto de ley.

Por último, se ha estimado conveniente precisar la gratuidad para el ejercicio de los derechos mencionados - salvo en los casos que establezca el reglamento -, así como los casos en que procede establecer límites al ejercicio de estos derechos derivados.

- Título V: Obligaciones del titular y del encargado del tratamiento del banco de datos personales

Pero los principios rectores de protección de los datos personales también tienen su expresión en las distintas obligaciones que incumben a los que efectúen su tratamiento. Así en este Título estos principios rectores se traducen en la obligación de efectuar el tratamiento de datos personales sólo previo consentimiento informado, expreso e inequívoco del titular de los datos personales; no recopilar datos personales por medios fraudulentos, desleales o ilícitos y recopilar sólo aquéllos que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido; no utilizar los datos personales objeto de tratamiento para finalidades distintas de aquéllas que motivaron su recopilación, salvo que medie procedimiento de disociación; almacenar los datos

---

[55] Nótese que los derechos de acceso, actualización, inclusión, rectificación, supresión y a impedir el suministro son reconocidos bajo tal denominación a través del Código Procesal Constitucional de 2004. En puridad, tienen el mismo alcance que los denominados derechos de acceso, rectificación y cancelación que son materia de diversa legislación sobre el tema.

[55] El ejercicio del derecho de oposición al tratamiento supone el tratamiento de datos sin consentimiento del titular. Conviene diferenciar esta figura de la revocación, pues aunque también se traduzca en el rechazo al tratamiento, tratándose de la revocación el tratamiento de datos personales se da por haber existido consentimiento previo, el que se decide retirar.

[57] Con el derecho al tratamiento objetivo, se pretende evitar que el tratamiento de datos personales permita o propicie actividades discriminatorias, lo que constituye una de las mayores preocupaciones frente al avance de la informática. Entre los datos que al efecto interesa proteger de este tratamiento tendencioso se encuentran los relativos al rendimiento laboral y a la situación crediticia, entre otros.

[58] El artículo 24° del proyecto de ley, sobre derecho a la tutela, establece la posibilidad de optar entre acudir a) a la Autoridad Nacional de Protección de Datos Personales en vía de reclamación, (artículos 219° y siguientes de la Ley N° 27444, Ley del Procedimiento Administrativo General), en cuyo caso, agotada la vía administrativa, procede recurrir al **Poder Judicial a través de la acción contencioso administrativa**; o b), alternativamente, acudir a la **acción constitucional de habeas data ante el Poder Judicial** (artículos 61° y siguientes del Código Procesal Constitucional). Ello resulta congruente con la regulación del habeas data que no exige el agotamiento de vía administrativa alguna – vía previa -, cuando ésta estuviere prevista (artículo 62°, parte final, del Código Procesal Constitucional).

personales de manera que se posibilite el ejercicio de los derechos de su titular; suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter incompleto o inexacto; suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo a que se sujetaría su tratamiento, salvo que medie procedimiento de disociación; así como proporcionar a la Autoridad Nacional de Protección de Datos Personales, la información relativa al tratamiento de datos personales que ésta le requiera y permitirle el acceso a los bancos de datos personales que administra, para el ejercicio de sus funciones.

Aunque no figuran incorporadas en este Título, a modo de ejemplo, también constituye obligación de los titulares y encargados de los bancos de datos personales adoptar medidas técnicas, organizativas y legales que garanticen la seguridad de los bancos de datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado; no crear bancos de datos que prescindan de las medidas de seguridad; así como guardar confidencialidad respecto del tratamiento de datos personales hasta aún después de finalizadas las relaciones que permitieron su conocimiento. Otras obligaciones se derivan del proyecto de ley y pueden ser establecidas en su reglamento.

- Título VI: Bancos de datos personales

Este Título se ocupa de los bancos de datos personales, tanto de administración pública como privada.

Al respecto, las primeras leyes sobre protección de datos posibilitaban sólo el control de los bancos de datos de administración pública. Posteriormente, pudo comprobarse que el peligro podía también proceder de bancos de datos de administración privada -como se ha graficado en la parte introductoria de este documento -.[59] En el proyecto de Ley, coincidiendo con lo advertido, se legisla la protección de datos a cargo de todos los bancos de datos personales, con independencia de su titularidad pública o privada[60].

En el proyecto de Ley se deja al desarrollo reglamentario la definición de las normas aplicables para la creación, modificación o cancelación de los bancos de datos. Adicionalmente, se establecen las reglas a que se sujetarán los servicios de tratamiento de datos personales prestados por terceros, así como los códigos de conducta a cargo de las entidades representativas de los titulares o encargados de bancos de datos personales de administración privada, los que tienen carácter de código deontológico o de buena práctica profesional.

---

[59] Cabe rescatar parte de las declaraciones emitidas por Artemi Rallo, Director de la Agencia Española de Protección de Datos (AEPD) en entrevista concedida al diario español "El País", edición del 28.11.2008: En cuanto al manejo estatal de este tipo de datos, Rallo tiene claro que su uso por el sector público no constituye una amenaza en comparación con su uso por el sector privado. "**La mayor parte de las inspecciones y sanciones impuestas por la agencia son a entidades privadas. En el 2007 frente a 66 sanciones a administraciones públicas se impusieron 399 a entidades privadas**". (Alfa Redi. Revista de Derecho Informático. Disponible en: http://www.alfa-redi.org/noticia.shtml?x=11137.) (Lo resaltado es nuestro).

[60] No obstante, cabe referir que la Ley de Protección de Datos Personales para el Distrito Federal de Méjico, de reciente publicación, regula únicamente los bancos de datos a cargo de entidades públicas.

- Título VII: Autoridad Nacional de Protección de Datos Personales

En este Título se desarrolla el régimen jurídico a que se sujeta la Autoridad Nacional de Protección de Datos Personales, condición que conforme a la opinión técnica especializada de la Secretaría de Gestión Pública de la Presidencia del Consejo de Ministros[61], recae en el Ministerio de Justicia, a través de la Dirección Nacional de Justicia, entidad que tendrá a su cargo realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones del proyecto de ley y de su reglamento.

Las funciones asignadas a la Autoridad Nacional de Protección de Datos Personales consideran funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras. Sus resoluciones son recurribles ante el Poder Judicial. Adicionalmente, se crea y norma el Registro Nacional de Protección de Datos Personales.

Refiriéndonos al Ministerio de Justicia, debemos señalar que se trata de un órgano del Poder Ejecutivo y ente rector del Sector Justicia que tiene por finalidad velar por la vigencia del imperio de la ley, el derecho y la justicia. Entre sus funciones se encuentra centralizar, coordinar, asesorar y promover la tutela y vigencia de los derechos humanos consagrados en la Constitución Política, las leyes y los tratados internacionales, función ésta ciertamente especializada y absolutamente necesaria para efectos de la plena eficacia de la ley que se propone y de la tutela efectiva del derecho fundamental a que ella refiere.[62] En consecuencia, la eficiencia y la eficacia que se requiere en la protección de datos personales en nuestro país se asegura designando al Ministerio de Justicia como Autoridad Nacional en tal materia.

En el desarrollo de la competencia asignada al Ministerio de Justicia y tal y como ha sido opinado por la Secretaría de Gestión Pública[63], la Oficina Nacional de Gobierno Electrónico e Informático (ONGEI) de la Presidencia del Consejo de Ministros, jugará un rol de apoyo y asesoramiento técnico, pues no en vano le corresponde brindar asistencia técnica a las entidades públicas en la implementación de los procesos de innovación tecnológica para la modernización de la administración. En efecto, téngase presente que la ONGEI es ente rector del Sistema Nacional de Informática, se encuentra encargado de implementar la Política Nacional de Gobierno Electrónico e Informática[64] y que actualmente, además, actúa como Secretaría Técnica de la Comisión Multisectorial para el Seguimiento y Evaluación del Plan de Desarrollo de la Sociedad de Información[65]. Para estos propósitos, en su oportunidad, se suscribirán los convenios de cooperación interinstitucional que correspondan.

---

[61] Informe N° 020-2009-PCM-SGP-LMA de la Secretaría de Gestión Pública remitido con Oficio N° 4007-2009-PCM/SG al Ministerio de Justicia.

[62] En efecto, véanse los artículos 4°, 5° y 6° inciso j) de Decreto Ley N° 25993, Ley Orgánica del Sector Justicia, así como los artículos 3° y 6° inciso d) del Reglamento de Organización y Funciones del Ministerio de Justicia aprobado pro Decreto Supremo N° 019-2001-JUS.

[63] Informe citado en el pie de página 61.

[64] A tal propósito, véase el artículo 49° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado por Decreto Supremo N° 063-2007-PCM.

[65] Al efecto, véase el Decreto Supremo N° 048-2008-PCM, Decreto Supremo que aprueba la reestructuración de la Comisión Multisectorial para el Seguimiento y Evaluación del "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana".

Si bien es cierto que, siguiendo el modelo europeo, habría sido conveniente crear una entidad con autonomía técnica, económica, presupuestal y administrativa a efectos que se desempeñe como Autoridad Nacional de Protección de Datos Personales, también lo es que la realidad de austeridad por la que atraviesa el país nos lo impide por el momento. En todo caso, esta decisión se adopta con la confianza en que con esta naturaleza jurídica inicial, la Autoridad Nacional de Protección de Datos Personales cumpla adecuadamente sus funciones y con ello sensibilice y ayude a la toma de conciencia de las autoridades y de la sociedad en general sobre la necesidad de brindar una adecuada protección a los datos personales.

Sin perjuicio de lo anterior, a efectos de procurar el fortalecimiento de la Autoridad Nacional de Protección de Datos Personales, se ha estimado conveniente establecer que constituirán recursos propios de ésta tanto las tasas por concepto de derecho de trámite de los procedimientos administrativos y servicios de su competencia, como los montos que recaude por concepto de multas y los recursos provenientes de la cooperación técnica internacional no reembolsable, entre otros.

- Título VIII: Infracciones y Sanciones Administrativas

Este Título se consagra a las infracciones y sanciones administrativas. Así, se clasifican las infracciones a las disposiciones del proyecto de ley como leves, graves y muy graves, derivando su tipificación al reglamento[66]. Igualmente, se establecen las sanciones que serán aplicables por la Autoridad Nacional de Protección de Datos Personales, sujetando su graduación a lo ya dispuesto en el artículo 230° numeral 3) de la Ley N° 27444, Ley del Procedimiento Administrativo General[67]. Se ha optado porque las sanciones administrativas sean de tipo económico. Estas multas han sido expresadas en Unidades Impositivas Tributarias (UIT) que pueden alcanzar inclusive las 100 (cien) UIT, a condición de que no se exceda el 10 % (diez por ciento) de los ingresos brutos anuales que hubiera percibido el presunto infractor durante el ejercicio anterior. Se considera la aplicación de multas coercitivas.

Finalmente, se ha previsto que la imposición de la multa se efectuará sin perjuicio de las sanciones disciplinarias sobre el personal de las entidades públicas en los casos de bancos de datos personales de administración pública, así como de la indemnización por daños y perjuicios y de las sanciones penales a que hubiera lugar.

- Disposiciones Complementarias Finales

Aunque no es lo usual y ya para finalizar, queremos comentar sólo dos Disposiciones Complementarias Finales, pues éstas merecen una reflexión aparte, sea por sus alcances o por su novedad.

Conforme a la Primera Disposición Complementaria Final, corresponderá al reglamento ocuparse de aspectos complementarios al proyecto de Ley o que se

---

[66] Ello al amparo de lo previsto en el artículo 230° inciso 4) de la Ley N° 27444, Ley del Procedimiento Administrativo General que permite la tipificación de las infracciones por la vía reglamentaria, si así se prevé por ley.

[67] Conforme a la Segunda Disposición Complementaria y Final de la Ley N° 27444, Ley del Procedimiento Administrativo General, sobre prohibición de reiterar contenidos normativos, las disposiciones legales posteriores no pueden reiterar el contenido de las normas de dicha ley, debiendo sólo referirse al artículo respectivo o concretarse a regular aquello no previsto.

estimen indispensables por motivos técnicos o para optimizar su cumplimiento[68]. Esto favorece su actualización constante, sin necesidad de recurrir a su modificación. Esta Disposición Complementaria Final debe aplicarse considerando el artículo 13°, numeral 13.2 del proyecto de ley, según el cual las limitaciones al ejercicio del derecho a la protección de datos personales sólo pueden ser establecidas por ley, deben respetar su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos.

Entre los temas que serán materia de necesaria reglamentación, a manera de ejemplo, citamos la determinación de las fuentes accesibles al público, el trámite aplicable a las solicitudes de los titulares de datos personales para el ejercicio de los derechos que la ley les reconoce, así como los requisitos que éstos deben cumplir a tal efecto; el régimen jurídico aplicable a la creación, modificación o cancelación de bancos de datos personales de administración pública y de administración privada; el régimen jurídico aplicable a la comercialización de datos personales y que luego serán empleados para fines publicitarios o en sistemas de promoción a distancia; el régimen especial a que se sujetará el tratamiento de los datos personales de los niños y de los adolescentes, así como las disposiciones específicas para la protección y garantía de sus derechos; el procedimiento de reclamación que se seguirá ante la Autoridad Nacional de Protección de Datos Personales por las actuaciones contrarias a lo dispuesto en la ley; las medidas cautelares y/o correctivas aplicables a los infractores de la ley; así como la tipificación de las infracciones, la escala de sanciones y el procedimiento para su aplicación, la regulación a que se sujetará la aplicación de las multas coercitivas; igualmente, el plazo para la adecuación de los bancos de datos personales creados con anterioridad a la ley, así como de sus reglamentos.

En la Cuarta Disposición Complementaria Final, se dispone la revisión de toda la normativa nacional para efectos de su adecuación a lo dispuesto en la ley, entiéndase, particularmente a sus principios rectores, sin perjuicio de la aplicación del test de proporcionalidad para el caso de las limitaciones que se estimen necesarias, siempre que éstas se efectúen mediante ley, no contravengan su contenido esencial y estén justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos.

Llegados a este punto y aunque por técnica legislativa no se indica en el proyecto, es indudable que la revisión que se ordena deberá iniciar con las normas con rango de ley vigentes actualmente, sea que se encuentren relacionadas con los bancos de datos de administración pública o con las fuentes de acceso público actualmente en funcionamiento, o con el tratamiento de las categorías de datos personales.

Para ilustrar lo anterior, queremos referirnos, por ejemplo, al caso de los sistemas de promociones a distancia que son materia de la 5ª Disposición contenida en el Anexo del Texto Único Ordenado de la Ley de Protección al Consumidor aprobado por Decreto Supremo N° 006-2009-PCM, según la cual los proveedores que empleen call centers, sistemas de llamado telefónico, de envío de mensajes de texto a celular o de

---

[68] En tal sentido resulta de utilidad revisar el Reglamento de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPRODA) que, por declaraciones de la Agencia Española de Protección de Datos, incrementaría la seguridad jurídica y contribuiría a conseguir una mayor claridad en la aplicación de la norma y a adaptar sus previsiones a la realidad existente. El Reglamento resolvería las cuestiones que se han planteado en la práctica consolidando y objetivando los precedentes de la Agencia, la Audiencia Nacional y el Tribunal Supremo.
Disponible en: http://www.hoytecnologia.com/noticias/Aprobado-Reglamento-Proteccion-Datos/37338

mensajes electrónicos masivos para promover productos y servicios, así como quienes presten el servicio de telemercadeo, deberán excluir de entre sus destinatarios a todos aquellos números telefónicos y direcciones electrónicas que hayan sido incorporados a una lista que para dicho fin implementará el INDECOPI. En dicha lista se podrán registrar los consumidores que no deseen ser sujetos de las modalidades de promoción antes indicadas.

En vinculación con lo señalado, nos referirnos a la Directiva de Operación y Funcionamiento del Registro de Números Telefónicos y Direcciones de Correo Electrónico Excluidos de ser Destinatarios de Publicidad Masiva (Registro "Gracias... No Insista")[69], especialmente polémica, por la cual se consagra el uso de los denominados "Ficheros Robinson" cuyos alcances - podrían sostener algunos - contravendrían los principios de consentimiento y finalidad[70]. En aplicación de la filosofía que subyace a estos ficheros – o lo que es lo mismo, bancos de datos - , la persona que no quiera ver mellada su privacidad por la recepción de propaganda no deseada, debe inscribirse en un banco de datos creado para tal efecto. Se invierte así la carga de la prueba y se termina beneficiando intereses privados comerciales.

Cabe señalar, en relación con este tema, que en artículo publicado en septiembre de 2008 bajo el título "El gobierno alemán endurecerá las leyes de protección de datos personales" se sostiene que luego de conocerse que los datos personales de los alemanes pueden comprarse fácilmente en Internet, el Ministro del Interior alemán, Wolfgang Schaeuble, ha señalado que se realizará una reforma de las leyes de protección de datos para hacerlas más estrictas. *"(...) **en el futuro las compañías sólo serán capaces de almacenar datos personales si los consumidores lo han acordado de forma específica**".*[71] (Lo resaltado es nuestro) Y es que las normas alemanas que ya existen permiten, por lo general, a los centros de llamadas y a otras compañías intercambiar direcciones personales a no ser que los consumidores digan que se oponen a ello.

Pero es importante anotar que conjuntamente con el mandato de revisión para adecuación, también se incluye el mandato de formulación de propuestas normativas específicas en caso de vacío o necesidad. En efecto, se considera que los alcances de la protección a los datos personales pueden completarse o precisarse, sobretodo en determinados sectores, a través de leyes particulares conforme a los principios rectores contenidos en este proyecto. Tal será el caso, por ejemplo, del tratamiento de los datos de salud de las personas, que ameritarán una regulación específica a cargo del Ministerio del ramo.

---

[69] Directiva N° 005-2009/COD-INDECOPI

[70] La **Declaración de Río de Janeiro del 2005**, suscrita por los representantes de América Latina y el Caribe, con ocasión de la Conferencia Regional Ministerial de América Latina y el Caribe preparatoria para la Segunda Fase de la Cumbre Mundial de la Sociedad de la Información, recoge la declaración siguiente: "8. Nuestro compromiso de reforzar la cooperación y la coordinación regional con el fin de **fomentar una cultura de ciberseguridad** que nos permite equilibrar la seguridad de la información y la seguridad de las redes con la privacidad y la protección del consumidor mientras se desarrollan nuevas aplicaciones. Este compromiso tiene el propósito de evitar el uso de las tecnologías y los recursos informativos con fines delictivos y terroristas, dentro de un marco de respeto de los derechos humanos y lucha contra el uso ilegal y el uso inadecuado de las TIC, entre otras cosas **contra el envío de correos electrónicos no solicitados, que podrían reducir la confianza de los usuarios o la estabilidad y la seguridad de los recursos y las redes de información.** (...)". (Lo resaltado es nuestro)

[71] Disponible en: http://www.hoytecnologia.com/noticias/Gobierno-aleman-endurecera-leyes/73950

Subyace a ambos mandatos (el de revisión para adecuación y el de formulación de nuevas propuestas legales) la opción por el desarrollo de legislación particular sectorial sobre datos personales[72], desestimando el desarrollo de una ley global, modelo actualmente adoptado, por ejemplo, por legislaciones como la chilena, paraguaya y uruguaya.

5. ACLARACION INDISPENSABLE

En ocasiones se ha sostenido que el derecho a la protección de datos personales constituye una barrera para la tutela de otros derechos fundamentales (libertad de información o acceso a la información) o de intereses públicos (desarrollo de la actividad económica). Frente a estos conflictos, la solución del problema no consiste en hacer prevalecer unos sobre otros[73]. En efecto, la solución pasa porque el juez aplique lo que nuestro Tribunal Constitucional ha denominado como la técnica de la ponderación, debiendo efectuarse un cuidadoso análisis en cada caso, a fin de evitar que el límite en la protección de uno de ellos sea en beneficio del ejercicio irrestricto (y abusivo) del otro[74].

En el proyecto de Ley no se adoptan pues fórmulas que privilegien ni uno ni otro derecho, como ocurre en la ley paraguaya, según la cual se dispone que la ley dictada en materia de protección de datos personales no se aplique a las libertades de emitir opinión y de informar[75], lo que en nuestra opinión cuestiona la efectividad de la tutela del derecho a la protección de datos personales frente al derecho a informar.

Es a través del silencio en esta materia y la consecuente aplicación de la técnica de ponderación desarrollada también a nivel doctrinario, que el proyecto busca armonizar las exigencias de información propias del Estado, con el ejercicio del derecho fundamental a la protección de datos personales. En todo caso y para que no quede duda al respecto, se ha cuidado de precisar que el uso de datos personales por parte de terceros debe realizarse en pleno respeto de los derechos fundamentales de sus titulares y de los derechos que esta ley les confiere.

---

[72] Acorde con la opción asumida, nótese que el 22º considerando de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" menciona que se ofrece a los Estados miembros de la Unión Europea la posibilidad de prever, independientemente de las normas generales, **condiciones especiales de tratamiento de datos en sectores específicos, así como para las diversas categorías de datos.** (Lo resaltado es nuestro)

[73] Tribunal Constitucional, op. cit., p. 73, L144, expediente Nº 1219-2003-HD, 21/01/04, S1, FJ.6.

[74] En la sentencia recaída en el expediente Nº 1797-2002-HD/TC del 29.01.2003, nuestro Tribunal Constitucional señala lo siguiente: "(...) Todos los derechos constitucionales tienen, formalmente, la misma jerarquía, por ser derechos constitucionales. De ahí que ante una colisión entre ellos, la solución del problema no consiste en hacer prevalecer unos sobre otros, sino en resolverlos mediante la técnica de la ponderación y el principio de concordancia práctica." (FJ Nº 11, 5º párrafo)
Disponible en: http://tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html

[75] Nos referimos a la Ley Nº 1969 que modifica, amplía y deroga varios artículos de la Ley Nº 1682/2001 "que reglamenta la información de carácter privado", artículo 1º.

ANALISIS COSTO - BENEFICIO

Las acciones necesarias para la aplicación de la ley se ejecutan con cargo al presupuesto institucional del pliego del Ministerio de Justicia, sin demandar recursos adicionales al Tesoro Público. Sin perjuicio de ello, cabe señalar que los costos para su implementación se restringen a los costos de operación de la Autoridad Nacional de Protección de Datos Personales. Estos costos desde ya se verán minimizados pues el Ministerio de Justicia cuenta con la infraestructura que se viene implementando a través de las Casas de la Justicia en todo el territorio nacional. En todo caso, conforme al artículo 36° del proyecto de Ley, se habilita una fuente de ingresos permanente a favor de la Autoridad Nacional de Protección de Datos Personales por las tasas y multas que está autorizada a cobrar.

Entre tanto, los beneficios de su vigencia son de gran alcance. Por un lado, el aseguramiento de mecanismos para el disfrute de un derecho fundamental reconocido en nuestra Constitución Política, pero poco difundido en sus alcances y pobremente exigido por sus titulares[76]; por otro lado, la posibilidad de aspirar a un nivel fluido de relaciones comerciales con la Unión Europea, pues en caso este proyecto de ley vea la luz – sin perjuicio de las normas adicionales y acciones paralelas que deban llevarse a cabo - , constituirá el documento base que podrá dar lugar a que la Unión Europea determine nuestra calificación como país con un nivel suficiente de protección de datos personales[77] [78], lo que dará paso al libre intercambio de datos personales con Europa que desde ya se traducirá en el incremento de inversiones en el Perú.[79] [80]. Esto que

---

[76] A pesar de su larga trayectoria en el tema, este problema no es ajeno a Europa. Así, en noticia difundida el 27.01.2008, el EUROPAPRESS reportó que en el 2003, más del 60 por ciento de los ciudadanos europeos tenía un conocimiento escaso acerca de sus derechos en materia de protección de datos y sobre la existencia de autoridades independientes con competencias para su protección. Atendiendo a esta situación, el Consejo, la Comisión Europa y todas las autoridades de protección de datos de los países miembros de la Unión Europea, promoverían para el día siguiente una jornada para celebrar el **Día Europeo de la Protección de Datos**, con el fin de impulsar, entre los ciudadanos europeos, el conocimiento de sus derechos y responsabilidades en esta materia y que se familiaricen con los aspectos normativos. (Lo resaltado es nuestro).
Disponible en: http://www.hoytecnologia.com/noticias/Proteccion-Datos-recibe-primeras/41557
El Día Europeo de Protección de Datos ha sido luego celebrado en los años 2009 y 2010.

[77] El procedimiento previsto por la Unión Europea para comprobar que un tercer país garantiza un nivel adecuado de protección de datos está regulado en el apartado 2 del artículo 25, del Capítulo IV, Transferencia de Datos Personales a Terceros Países de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" y a la letra señala lo siguiente: "El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos en el país de origen y el país de destino final, las normas de Derecho, generales y sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países."

[78] "Como regla general, podrá considerarse que el Estado otorga un nivel de protección adecuado en los supuestos en los que el mismo cuente con una norma reguladora de la protección de datos que contenga los principios sustantivos que se han enumerado y exista una autoridad encargada de velar por su cumplimiento, ante la cual los ciudadanos puedan dirigir sus reclamaciones y que ostente poderes de inspección e investigación de los tratamientos. (Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana elaborado por la Red Iberoamericana de Protección de Datos, p.11.)

[79] Mediante la Decisión de la Comisión de 30 de junio de 2003, la Unión Europea ha reconocido a la normatividad argentina como adecuada en los términos de la Directiva N° 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 "relativa a la protección de las personas físicas en lo

sostenemos respecto de Europa también sería aplicable en nuestra relación con las economías miembro del APEC que actualmente cuentan con similares dispositivos de control del tráfico de datos personales.

EFECTO DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La promulgación del proyecto de Ley generará un impacto positivo en el sistema jurídico peruano, al establecer el marco especial aplicable en materia de tratamiento de datos personales. A partir de su vigencia, corresponderá la revisión integral de la normativa existente a efectos de su adecuación y, de ser el caso, la dación de leyes particulares sectoriales según los datos de que se trate.

---

que respecta al tratamiento de datos personales y a la libre circulación de estos datos". Este reconocimiento significa la no aplicación a Argentina de restricciones para la transferencia de datos personales, permitiendo el libre flujo de los datos personales desde la Unión Europea a dicho país.

[60] Es pertinente, en tal sentido, referirnos al negocio de los Call Centers, entendidos éstos como centros de contacto de nueva generación que son utilizados por las empresas para vender sus productos o servicios y manejar las relaciones con sus clientes, en actividades como asesoría, información, asistencia técnica, investigación y cobranzas. Según cifras al 2009, existen más de 60 empresas con 20 mil posiciones instaladas y disponibles en el Perú, lo que genera aproximadamente 40 mil empleos directos ya que hay dos turnos diarios. Se estima que al 2012 se generarán 75 mil empleos, cifra que ciertamente crecería por efecto de la inversión particularmente europea, que sea motivada por un marco regulatorio específico que provea de confidencialidad y seguridad a los datos de los clientes de los proveedores europeos de estos servicios. Ciertamente, frente a otros países latinoamericanos, el Perú ya presenta importantes ventajas competitivas para el desarrollo del negocio de los Call centers (menos costo de mano de obra y flexibilidad laboral, tono de voz neutral, requerimientos tecnológicos, costos menores alquiler de locales o de costo de viviendas, exención del IGV a la exportación de servicios de Call Centers). Si a ello agregamos la dación de una ley específica, el crecimiento de la inversión extranjera por encima de las cifras a la fecha proyectadas resulta seguro. (Fuente: PROINVERSION)