RED ACADÉMICA INTERNACIONAL DE

PROTECCIÓN DE DATOS PERSONALES

RIPDP

Revista Internacional de Protección de Datos Personales

El marco normativo latinoamericano y la ley de protección de datos personales del Perú

Ma. de Lourdes Zamudio Salinas

Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia)
No. 1 Julio - Diciembre de 2012. ISSN: 2322-9705

El marco normativo latinoamericano y la ley de protección de datos personales del Perú

Ma. de Lourdes Zamudio Salinas*

Resumen

América Latina en cuanto a la regulación del derecho a la protección de datos personales sigue un ritmo propio; el mismo que se expresa en diversas características cuya conceptualización se propone en el presente artículo. Se sustentará cómo en Latinoamérica la legislación sobre la materia ha evolucionado significativamente en los años que van corriendo en este nuevo milenio, presentando las leyes de carácter general con autoridades de control aprobadas en cinco países. De igual forma, se desarrollarán las dos vías jurídicas que de manera complementaria los países latinoamericanos han utilizado para la protección de los datos personales: la de los tratados y la de la legislación interna. Se expondrá el marco normativo de la protección de datos personales en el Perú, previo a la dación de su Ley N° 29733, publicada en julio de 2011,

Abstract

Latin America in terms of regulate the right of protection of personal data follows its own rhythm, the same that is expressed in various features whose conceptualization is proposed in this article. It will be based on how Latin America has evolved significantly in the legislation of the subject over the years in this new millennium, presenting the general laws with authorities of control, approved in five countries. Similarly, the two legal ways will be developed, the ones that in a complementary way Latin American countries have used in order to protect personal data: the one of the treaties and the one of domestic legislation. It will be presented in a legal framework for the protection of personal data in Peru prior to the enactment of Law No. 29,733, published in July 2011, general rule that has

* Abogada por la Universidad de Lima. Maestría en Derecho Constitucional por la Pontificia Universidad Católica del Perú. Catedrática asociada de la Facultad de Derecho y de la Escuela de Negocios, en la Universidad de Lima. Experta de la Red Iberoamericana de Protección de Datos y miembro de la Red Académica Internacional de Protección de Datos. Se ha desempeñado como asesora en materia constitucional de diversas autoridades peruanas, tales como presidentes de Consejos de Ministros, ministros de Justicia y de la fiscal de la Nación, así como consultora en materia constitucional para diversas instituciones del Estado. Exagente del Estado peruano ante la CDH. Ha publicado diversos artículos sobre el tema de derechos humanos. Correo electrónico: mariadelourdes.zamudio@gmail.com

norma de carácter general y que ha diseñado una autoridad de control administrativa. Dicha norma será desarrollada en varios de sus aspectos principales.

Palabras claves: Protección de datos personales, América Latina, marco normativo, transferencias internacionales, privacidad, legislación interna, constitución, hábeas data, ley de protección de datos, autoridad nacional de protección de datos personales, banco de datos, responsable del tratamiento.

designed an administrative authority of control. This rule will be developed in several of its main aspects.

Keywords: Protection of personal data, Latin America, Legal Framework, International transfers, Privacy, Internal legislation, Constitution, Hábeas Data, Data Protection Act, National Authority of Personal data protection, Data bank, The controller.

Sumario

Introducción - I. MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS - *A. Instrumentos supranacionales* - 1. Instrumentos internacionales de carácter general - 2. Instrumentos internacionales que involucran a Estados latinoamericanos y que contienen disposiciones sobre privacidad e intimidad - 3. Instrumentos subregionales o bilaterales - *B. Legislación interna* - 1. Situación de asimetría normativa - 1.1 Estados con ley de protección de datos personales de carácter general y con autoridad de control administrativa - 1.2 Estado con protección legislativa general pero sin autoridad de control administrativa - 1.3 Estados con reconocimiento constitucional explícito del derecho a la protección de datos personales - 1.4 Estados con reconocimiento constitucional explícito del recurso del hábeas data - 1.5 Estados con reconocimiento constitucional explícito del derecho a la intimidad y a la privacidad - 2. Consideración política del tema a nivel regional - 3. Prevalencia inspiradora del modelo europeo - II. LA PROTECCIÓN DE DATOS PERSONALES EN EL PERÚ. LA LEY N° 29733 - *A. Nivel constitucional - B. Ley de protección de datos personales. Ley N° 29733* - 1. Objeto de la Ley - 2. Definiciones - 3. Ámbito de aplicación - 4. Tratamiento de datos personales - 5. Principios rectores - 6. Derechos del titular de datos personales - 7. Flujo transfronterizo de datos personales - 8. Autorregulación - 9. Autoridad Nacional de Protección de Datos Personales - III. CONCLUSIONES - Bibliografía.

Introducción

El derecho a la protección de datos personales, que empezó a gestarse de manera autónoma en el contexto europeo, comienza a introducirse en América Latina a través de la institución del hábeas data, en la década del 90. De igual modo, constituciones políticas de algunos Estados latinoamericanos comenzaron a incorporar este derecho, principalmente a partir de la primera década del presente milenio. Durante este mismo lapso, sumado a los años que nos llevan hasta el presente 2012, la regulación sobre dicha materia ha evolucionado significativamente, traduciéndose en la aprobación de diversas leyes de carácter general con autoridades de control. No obstante lo señalado, existe una gran diversidad en la forma y en el nivel de protección con la que Latinoamérica ha atendido a este derecho.

Son diversas las manifestaciones que expresan que la protección de los datos personales todavía no es la adecuada en esta región, pues no está a la altura de los desafíos que supone el tratamiento de los datos de las personas mediante el uso de las tecnologías de la información y de las comunicaciones dentro de un mundo globalizado.

En el contexto planteado es importante y, por lo tanto, parte de los objetivos del presente estudio, conocer el desarrollo del marco normativo de la protección de datos en los países latinoamericanos, conceptualizando sus principales características y categorizando las opciones legislativas que los países de esta región han seguido en la materia.

De igual modo, se pretende hacer una presentación de la Ley peruana de protección de datos personales, Ley Nº 29773 del 2011, la cuarta que se aprueba en un país latinoamericano como ley general sobre la materia con una autoridad de control. Sobre este particular, se comenzará explicando el diseño jurídico de la protección de datos personales en el Perú desde antes de la Ley N° 29733, incluyendo aspectos relevantes de esta norma, para concluir con la identificación de su principal reto con miras a que su legislación sea efectiva.

Para el logro de los objetivos planteados se ha analizado, principalmente, la normativa de diversos países de América Latina en materia de derechos fundamentales incluida en sus constituciones políticas, así como las leyes de protección de datos personales de los países que correspondan; igualmente se ha utilizado tratados sobre la materia, así como documentos elaborados por la Red Iberoamericana de Protección de Datos.

Con la Ley de protección de datos personales, Ley N° 29733, publicada el 03 de julio de 2011, el Perú se suma en América Latina a la lista corta, pero significativa, de países que como Argentina (2000), Uruguay (1998), México (2010), Costa Rica (2011) y Nicaragua (2012), han aprobado leyes generales de protección de datos personales.[1] En el presente artículo analizaremos la tendencia normativa en materia de protección de datos en Latinoamérica para desembocar en

1 La ley colombiana, aprobada por el Congreso de la República en el 2010, no está aún sancionada, pues por tratarse de una ley estatutaria se encuentra en análisis de constitucionalidad en la Corte Constitucional de ese país, organismo que hasta la fecha (junio del 2012) no ha emitido la sentencia respectiva.

la realidad legislativa peruana que se concretó en su Ley Nº 29773 del 2011.

I. MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS[2]

La protección de datos en América Latina presenta diversas características, las mismas que de manera dinámica configuran la forma como los países de esta región han ido regulando esta materia. En el I Foro internacional sobre protección de datos personales, UANL,[3] al analizar el tema vemos que, a diferencia de lo que sucedió en Europa, en donde ya encontramos desarrollos normativos en la década del setenta, en la región latinoamericana solo hasta la década del ochenta se comienza a discutir sobre la materia y el tema de la protección de datos se introduce a finales de ella a través de la institución del hábeas data que se difunde en los años noventa. En cuanto a la regulación del derecho a la protección de datos personales, América Latina sigue su ritmo propio. Un ritmo que se debe, entre otras razones, a que los legisladores, en la mayoría de estos países, tienen un nivel medio-regular de conocimiento sobre la materia; a los episodios de interrupción constitucional en varios Estados; y al hecho de que este tema no suele ser una prioridad en la agenda política de la mayoría de las autoridades correspondientes. Los Estados latinoamericanos, en el desarrollo de esta materia, como en otras, han venido evolucionando y respondiendo dentro de su propio contexto.

La regulación sobre la protección de datos personales que está desarrollándose en América Latina y que puede calificarse como importante durante los años que han corrido en este nuevo milenio, responde a varias razones: una, y probablemente la más efectiva, es la que nos impone la globalización económica, en virtud de la cual resulta imprescindible buscar un equilibro entre los intereses económicos —que cada vez más exigen mayores transferencias internacionales de datos, a la par que un tratamiento adecuado de ellos, pues su protección constituye un derecho fundamental de la persona— para que el desarrollo del comercio internacional sea compatible con una adecuada protección de la privacidad en lo que respecta a los datos personales.

En este cometido, las vías jurídicas que los países latinoamericanos han utilizado para lograr ese equilibrio son varias y complementarias. Mencionamos dos, que desarrollaremos sin la intención de ser exhaustivos: los instrumentos supranacionales y la legislación interna.

A. Instrumentos supranacionales

Esta vía, conformada por las declaraciones, recomendaciones y tratados la hemos clasificado como sigue:

1. Instrumentos internacionales de carácter general

Buscan establecer los principios fundamentales que sirvan de base para la adopción de instrumentos internacionales sobre protección de datos personales. Entre otros, encontramos los

2 "A junio de 2012."

3 Monterrey, 04-05 de octubre del 2010, Universidad Autónoma de Nuevo León.

siguientes: ONU (Resolución 45/95. Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales), OCDE (Organización para la Cooperación y el Desarrollo Económico: directivas relativas a la protección de la privacidad y flujos transfronterizos de datos personales), Acuerdo general sobre comercio en servicios (GATS), artículo XIV- c - ii. Marco de los tratados OMC, APEC (Foro de Cooperación Asia-Pacífico: Marco de privacidad).

2. Instrumentos internacionales que involucran a Estados latinoamericanos y que contienen disposiciones sobre privacidad e intimidad

Estos instrumentos no se refieren necesariamente a datos personales, pero como el derecho a la protección de datos personales se desprende y autonomiza del derecho a la intimidad, sirven de sustento jurídico para alcanzar su tutela vía los órganos jurisdiccionales competentes; así como para sustentar el desarrollo del mismo a la hora de emprender una tarea legislativa. Dentro de éstos encontramos los siguientes: Declaración Universal de los Derechos Humanos (1948), artículo 12; Declaración Americana de los Derechos y Deberes del Hombre (1948), artículo 5; Pacto Internacional sobre Derechos Civiles y Políticos (1966), artículo 17; Convención Americana sobre Derechos Humanos (1969), artículo 11; Convención de Derechos del Niño (1989), artículo 16.

3. Instrumentos subregionales o bilaterales

En este punto, a modo de ejemplo, podemos citar el tratado de libre comercio celebrado entre Perú y los Estados Unidos de América, numerales 3 y 4 del artículo 14.2 sobre acceso y uso de los servicios públicos de telecomunicaciones, del Capítulo 14°, Telecomunicaciones (febrero del 2009); el tratado de libre comercio suscrito entre Perú y Canadá (agosto del 2009), que a modo de compromiso de mejores esfuerzos tiene el artículo 1507 referido a la protección de la información personal. Asimismo, el compromiso asumido en el marco del Plan de Acción Regional del eLAC 2007 para la sociedad de la información, a través de su meta 25[4] y el Plan de Acción del eLAC 2010 a través de su meta 78.

B. Legislación interna

La legislación interna de los países de América Latina que consagra y garantiza el contenido esencial del derecho a la protección de datos personales constituye, para nosotros, la segunda vía que complementa a la de los instrumentos supranacionales; vías a través de las cuales los países latinoamericanos están construyendo su sistema de protección de datos personales.

A continuación señalamos solo tres características de la regulación protectora de los datos

4 "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."

personales en América Latina, en adelante AL, las cuales hemos conceptualizado como sigue: situación de asimetría normativa; consideración política del tema a nivel regional; y prevalencia inspiradora del modelo europeo.

1. Situación de asimetría normativa

En América Latina la atención normativa del derecho a la protección de datos personales es asimétrica. La mayoría de los Estados latinoamericanos reconocen el derecho a la protección de datos personales por referencia directa de su Constitución o como consecuencia de las decisiones adoptadas por sus órganos jurisdiccionales, fundamentalmente por medio del reconocimiento de la acción[5] del hábeas data, mediante la cual el titular tiene derecho a conocer los datos referidos a sí mismo y la finalidad para la que están siendo tratados por un determinado responsable, pudiendo en su caso instar su rectificación, cancelación o actualización. El ejercicio de este derecho a través del hábeas data ha dado lugar a una rica jurisprudencia que ha evolucionado hacia el reconocimiento de una serie de principios a los que debe someterse todo tratamiento de datos personales sea dentro del ámbito de la administración pública como de la privada.[6]

Hemos catalogado en cinco clases a los países de nuestra región, en atención a la forma en que han normado la protección de los datos personales en sus legislaciones internas:

1.1 Estados con ley de protección de datos personales de carácter general y con autoridad de control administrativa. En esta clase se encuentran:

Argentina, con su Ley N° 25326, Ley de protección de los datos personales, sancionada el 4 de octubre del 2000 y posteriormente reglamentada por el Decreto N° 1558/2001. Único país latinoamericano al que la Comisión Europea consideró que ofrecía un nivel de protección adecuado (Decisión 2003/490/CE de 30 de junio de 2003). Su órgano de control está constituido por la Dirección Nacional de Protección de Datos Personales que se encuentra dentro del ámbito del Ministerio de Justicia, Seguridad y Derechos Humanos.

Uruguay, con su Ley N° 18331, de protección de datos personales y acción de hábeas data, del 11 de agosto 2008, reglamentada por el Decreto Nº 414/009 de 31 de agosto del 2009. Tiene como órgano de control a la Unidad Reguladora y de Control de Datos Personales, ente desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC).

México, con su Ley federal de protección de datos personales en posesión de los particulares, publicada el 5 de julio del 2010 y reglamentada mediante norma del 21 de diciembre del 2011. El IFAI, Instituto Federal de Acceso a la Información y Protección de Datos es el órgano de control que suma a sus funciones de velar por el derecho fundamental de acceso a la información pública y de protección de datos personales en posesión del sector público, la de la protección de los datos personales en posesión de particulares.

5 Recurso o proceso constitucional.

6 Directrices para la armonización de la protección de datos en la Comunidad Iberoamericana de Protección de Datos. 2007.

Perú, con su Ley N° 29733, publicada el 03 de julio del 2011, tiene como autoridad de control a la Dirección General de Protección de Datos Personales bajo el ámbito de competencia del Ministerio de Justicia y Derechos Humanos.[7]

Costa Rica, con su Ley de protección de la persona frente al tratamiento de sus datos personales N° 8969, publicada el 05 de setiembre del 2011. Su autoridad de control es la Agencia para la Protección de Datos Personales (PRODAT).

Nicaragua, con su Ley N° 787, publicada el 29 de marzo del 2012.

1.2 Estados con protección legislativa general pero sin autoridad de control administrativa. En esta clase se ubica solo Chile, con su Ley Nº 19628 sobre protección de la vida privada, publicada el 28 de agosto de 1999.

1.3 Estados con reconocimiento constitucional explícito del derecho a la protección de datos personales. Dentro de esta clase encontramos a países como México, artículo 6; Panamá, artículo 41 A; Perú, artículo 2, inciso 6; y Venezuela, artículo 28.

1.4 Estados con reconocimiento constitucional explícito del recurso del hábeas data: Bolivia, artículo 23; Panamá, artículo 44 C; Perú, artículo 200, inciso 3; Colombia, artículo 15[8]; Brasil, artículo 5, LXXII; Ecuador, artículo 94; Honduras, Decreto Legislativo N° 381-2005.[9]

1.5 Estados con reconocimiento constitucional explícito del derecho a la intimidad y a la privacidad. Dentro de los Estados con reconocimiento constitucional explícito del derecho a la intimidad y a la privacidad, pero no de protección de datos personales, encontramos a países como Brasil, artículo 5, X; Ecuador, artículo 23; El salvador, artículo 2 y Honduras, artículo 76.

En los Estados que no tienen expresamente reconocido el derecho a la intimidad o el específico de la protección de datos personales, se sostiene que sí existe dicha protección de manera implícita a través de la denominada cláusula de *números apertus* de los derechos humanos contenida en diversos textos constitucionales, o de la integración de los principios consagrados en los tratados internacionales, ratificados por cada país, como parte del ordenamiento jurídico nacional. En estos países, así como en los comprendidos en el subacápite 1.5, puede hacerse valer el derecho a la protección de datos personales jurisdiccionalmente a través del recurso general del amparo.

No obstante lo señalado, en la legislación infra constitucional la tendencia normativa que todavía sigue la mayoría de los países latinoamericanos está constituida por la legislación sectorial que se encuentra dispersa en los ordenamientos jurídicos; en este sentido, encontramos disposiciones relativas a la protección de datos personales en leyes sobre materias referidas a: las centrales privadas de información crediticia; transparencia y acceso a la información pública; protección al consumidor; telecomunicaciones; salud; sistema estadístico; sistema de identificación de las personas; correo no deseado

7 A la fecha , junio del 2012.

8 Pero como derecho fundamental.

9 Bolivia. Constitución Política de 2009.

La vigente CPE considera la Acción de Protección de Privacidad en el artículo 130, que en la abrogada Constitución estaba establecido en el artículo 23 como Recurso de Hábeas data.

(spam); penal; niños, niñas y adolescentes; y tributaria, entre otras.

2. Consideración política del tema a nivel regional

En América Latina ya existe un reconocimiento del tema al más alto nivel, contenido en el parágrafo 45 de la Declaración de la XIII Cumbre Iberoamericana de Santa Cruz de la Sierra, (Bolivia), emitida por los Jefes de Estado y de Gobierno de veintiún países iberoamericanos (noviembre del 2003). Declaración de Santa Cruz de la Sierra:

45. Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad.

Si bien esta declaración es política, sirve de base para la sustentación de los correspondientes desarrollos normativos en Latinoamérica.

3. Prevalencia inspiradora del modelo europeo

Teniendo en cuenta las leyes de protección de datos de carácter general aprobadas en los países latinoamericanos, resulta bastante claro y explícito por lo expresado en varias de las exposiciones de motivos correspondientes y por la opción legislativa desarrollada, que estas han tenido como fuente de inspiración el modelo europeo. Sustenta lo señalado el hecho de tomar como bases, entre otros documentos, el Convenio 108 del Consejo de Europa del 1° de octubre de1985 para la protección de las personas con respecto al tratamiento automatizado de los datos personales y su Protocolo Adicional de 2001; la Directiva Comunitaria 95/46/CE del Parlamento Europeo y del Consejo del 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 la Ley orgánica 15/1999 de protección de datos de carácter personal española. Asimismo, se suele sostener a la hora de sustentar los proyectos de leyes generales[10] la conveniencia de institucionalizar la transferencia internacional de datos entre Europa y AL buscando la declaración de la Comisión Europea de ser considerado un país con destino adecuado. Se suma a estos hechos la actuación de la Red Iberoamericana de Protección de Datos, creada en el 2003 en Guatemala, que congrega a más de veintidós países de la región y que se ha constituido en un foro importante de reflexión, discusión, difusión y asesoramiento para todos los Estados latinoamericanos que emprenden una regulación sobre la materia.

Dentro del contexto, no exhaustivo, presentado sobre las opciones legislativas en materia de protección de datos, surge la pregunta: ¿Es conveniente que la asimetría normativa en materia de regulación de la protección de datos personales existente en América Latina sea superada?

10 De los países con las leyes de carácter general mencionados.

Si se considera que estamos en un mundo global, con un mercado globalizado[11], y pretendemos que esto funcione de manera equilibrada, a la luz del respeto por la persona humana y sus derechos fundamentales, creemos necesario que los desarrollos normativos de los países latinoamericanos deben darse de manera armónica y a través de políticas de largo alcance. Por lo expuesto, consideramos que el camino en este sentido ya se ha iniciado y que debemos seguir avanzando hacia soluciones coordinadas en materia de protección de los datos personales, buscando soluciones integradas en los aspectos que lo ameriten, pero adecuando lo que corresponda a cada realidad. Esto supone entender como normal la existencia de aspectos particulares propios en cada uno de los Estados, lo que se traduce en la presencia de instituciones sobre la materia con rasgos particulares. No obstante lo señalado, no se debe dejar de tener en cuenta que la persona humana, en su dignidad, tiene la misma naturaleza cualquiera sea la realidad estatal de que se trate y, por lo tanto, le corresponden los mismos derechos, aunque hoy en día se mueva y desarrolle globalmente con particulares desafíos.[12]

A continuación presentamos la protección de datos personales en el Perú, con énfasis en la Ley de protección de datos, norma que ha tomado como base la legislación europea y específicamente la española.

II. LA PROTECCIÓN DE DATOS PERSONALES EN EL PERÚ. LEY N° 29733

El marco normativo[13] de la protección de datos personales en el Perú, hasta antes de la dación de la Ley N° 29733, se venía dando por una serie de normas jurídicas de distinto nivel jerárquico, dispersas en todo el ordenamiento jurídico.

A. Nivel constitucional

La Constitución Política de 1993 establece los derechos que constituyen la fuente primigenia que marca e inspira la legislación existente sobre protección de datos personales. En este acápite nos referiremos no solo a lo expresamente dispuesto por la Constitución Política, sino que haremos referencia a las otras disposiciones que constituyen el bloque de constitucionalidad, como son el Código Procesal Constitucional y las sentencias del Tribunal Constitucional.

El artículo 2°, inciso 7) de la Carta Constitucional reconoce los derechos a la intimidad, al honor y a la propia imagen, que ya se encontraban consagrados en la Constitución Política de 1979. En el mismo artículo 2°, pero en el inciso 6), se reconoce un nuevo derecho, cuando señala que los servicios informáticos, computarizados o no,

11 Que hacen necesarios el uso de servicios web como el comercio electrónico y la computación en nube, entre otros.

12 En junio del 2011 se presentó en la OEA el documento *Principios y recomendaciones preliminares sobre la protección de datos personales*, preparado de conformidad con la resolución AG/RES. 2514, que busca servir de base para un futuro instrumento internacional sobre la materia. Ver documento en http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf

13 Zamudio Salinas, M. de L., "Perú: La protección de datos personales". En *Lumen,* revista de la Facultad de Derecho de la Universidad del Sagrado Corazón, N° 7, enero a diciembre del 2010, Lima, 2010, pp. 127-135.

públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. El Tribunal Constitucional definió este derecho como el de autodeterminación informativa, en su sentencia de fecha 29 de enero de 2003, expediente Nº 1797-2002-HD/TC, en el marco de un proceso de hábeas data.[14]

A su vez, el artículo 200º, inciso 3) de la Constitución Política de 1993, establece la Garantía Constitucional del hábeas data para proteger los derechos reconocidos en los incisos 5), derecho de acceso a la información pública, y 6) derecho a la protección de datos personales, del artículo 2º de la Carta fundamental.

La Ley Nº 28237 que aprobó el primer Código Procesal Constitucional (CPC) peruano, en vigor desde el 01 de diciembre del 2004, en su artículo 61, inciso 2), establece que toda persona puede recurrir al proceso de hábeas data para

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

Hasta el cuatro de julio de 2011[15], el único instrumento de tutela del derecho a la protección de datos personales en el Perú era la acción de hábeas data; con la Ley de protección de datos personales, Ley N° 29733, en adelante el derecho a la protección de datos personales es desarrollado legislativamente y se crea una autoridad de control, que se suma a la tutela jurisdiccional existente en el hábeas data, pero ya en el ámbito administrativo y que se espera sea más efectiva y rápida.

B. Ley de protección de datos personales. Ley N° 2973

Esta novísima norma de desarrollo constitucional tiene un título preliminar y siete títulos comprendidos en cuarenta artículos, así como doce disposiciones complementarias finales. A continuación presentamos esta ley en algunos[16] de sus aspectos relevantes. Esta norma, recién está siendo materia de real asimilación y toma de conciencia por la mayor parte de la academia, de las autoridades y de la sociedad en general en el Perú.

14 "El derecho reconocido en el inciso 6) del artículo 2° de la Constitución es denominado por la doctrina *derecho a la autodeterminación informativa,* y tiene por objeto proteger la intimidad personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les (sic) conciernen". (Expediente Nº 1797-2002-HD/TC en un proceso de hábeas data).

15 Disposiciones complementarias finales. "Duodécima. Vigencia de la Ley. La presente Ley entra en vigencia conforme a lo siguiente: 1. Las disposiciones previstas en el Título II, en el primer párrafo del artículo 32 y en las primera, segunda, tercera, cuarta, novena y décima disposiciones complementarias finales rigen a partir del día siguiente de la publicación de esta Ley. (…)"

16 En atención a los límites que establecen la naturaleza del presente artículo.

1. Objeto de la Ley. Está definido de manera directa y simple en el artículo 1°. Consiste en garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2, numeral 6 de la Constitución Política de 1993.[17] Con esta declaración se "coloca" legalmente el epígrafe al citado numeral constitucional, definido en algunas oportunidades por la jurisprudencia del Tribunal Constitucional como el derecho a la autodeterminación informativa. La ley señala que la garantía del derecho fundamental a la protección de los datos personales se materializará a través de un adecuado tratamiento de los mismos en un marco de respeto de los demás derechos fundamentales que en la Constitución se reconocen.

El marco de garantía del derecho que nos ocupa se delimita entonces por el respeto a los demás derechos fundamentales que la Carta Política del Perú reconoce, en lo cual es bastante amplia, pues además de la lista contenida en los veinticuatro incisos del artículo 2°, incluye la denominada cláusula de *números apertus* de los derechos fundamentales (artículo 3°) y la cláusula interpretativa de los derechos, que hace parte de la cuarta disposición final y transitoria[18], y que remite para la interpretación de las normas relativas a los derechos y a las libertades, a la Declaración Universal de Derechos Humanos, así como a los tratados y acuerdos internacionales sobre las mismas materias ratificados por el Perú.

2. Definiciones. La Ley, en su artículo 2°, define los siguientes conceptos: banco de datos personales, banco de datos personales de administración privada, banco de datos personales de administración pública, datos personales, datos sensibles, encargado del banco de datos personales, entidad pública, flujo transfronterizo de datos personales, fuentes accesibles para el público, nivel suficiente de protección para los datos personales, persona jurídica de derecho privado, procedimiento de anonimización, procedimiento de disociación, titular de datos personales, titular del banco de datos personales, transferencia de datos personales y tratamiento de datos personales. El artículo concluye habilitando al reglamento de la ley para realizar un mayor desarrollo de las definiciones existentes.

Datos personales. La ley define como datos personales a toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados. De la definición se desprende que pueden ser datos que correspondan al ámbito de la privacidad, así como al más restringido de la intimidad.

Datos sensibles. Esta categoría especial de datos personales estaría constituida por los siguientes: datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos;

17 Art. 2.- Toda persona tiene derecho a: (…) 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

18 Cuarta.- Interpretación de los derechos fundamentales

Las normas relativas a los derechos y a las libertades que la Constitución reconoce se interpretan de conformidad con la Declaración Universal de Derechos Humanos y con los tratados y acuerdos internacionales sobre las mismas materias ratificados por el Perú.

opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; información relacionada a la salud; e información relacionada a la vida sexual. Nos cuestionamos sobre la incorporación genérica como datos sensibles, de los ingresos económicos, no encontrando antecedente sobre el particular en la legislación comparada. Creemos que los ingresos económicos al tener la calidad de datos personales tienen la protección legal establecida por los principios y disposiciones de la Ley, pero darles la categoría de sensibles puede constituir un exceso, pues estos datos no tienen una naturaleza equivalente a la de otros, como el origen racial y étnico, la información relacionada a la salud o a la vida sexual, por ejemplo. En la exposición de motivos no hay ningún comentario sobre esta incorporación. Cabe precisar que, dentro de los ingresos económicos que no se considerarán sensibles, se encuentran los ingresos de los funcionarios y servidores públicos a que se refiere la Constitución Política del Perú en su artículo 41, así como la Ley que regula la publicación de la declaración jurada de ingresos, y de bienes y rentas de los funcionarios y servidores públicos del Estado (Ley N° 27482). De otro lado, el artículo 2°, inciso 5) de la Carta Fundamental protege el secreto bancario y la reserva tributaria.

Titular de datos personales. El legislador peruano ha optado por circunscribir a la persona natural al ámbito de protección de la Ley, excluyendo a las personas jurídicas o morales; el titular será la persona natural a quien correspondan los datos personales.

Titular del banco de datos personales[19]. Será la persona natural o jurídica que determina la finalidad y el contenido del banco de datos personales, así como el tratamiento de estos y las medidas de seguridad que correspondan. La ley peruana no incorpora la figura del responsable del fichero o del tratamiento, como sí lo hacen por ejemplo los artículos 3, literal d) de la ley española; artículo 4, literal K de la ley uruguaya, y el artículo 3, numeral XIV de la ley mexicana. En sentido similar, la Resolución de Madrid de 2009, reconocida como el primer esfuerzo para establecer estándares internacionales sobre la materia, incorpora la expresión responsable del tratamiento de datos, como la persona natural o jurídica, pública o privada, que por sí misma o en asociación con otros, decida sobre la base de datos o el tratamiento de los datos. Consideramos que la figura del responsable del tratamiento es un concepto más amplio que abarca tanto al titular del banco de datos como a quien decida sobre el tratamiento de datos personales, independientemente de que sea el titular del banco de datos o de que los datos consten o no en un banco. El proyecto de reglamento de la Ley publicado el 03 de marzo de 2012 incorpora dentro de las definiciones a la figura del responsable del tratamiento como aquel que decida sobre el tratamiento de datos personales, aún cuando no se encuentren en un banco de datos (artículo 2°, inciso 3). Coexistirían entonces para la ley peruana la figura del titular del banco de datos con la del responsable del tratamiento, aplicándose este último cuando el

19 La denominación utilizada por la ley difiere de otras como la usada por la Directiva 95-46-CE que se refiere al responsable del tratamiento, en su artículo 2° literal d).

titular de un banco de datos no decida sobre el tratamiento de los mismos o, de ser el caso, estos no se encuentren en un banco de datos y sean sometidos a tratamiento.

Nivel suficiente de protección para los datos personales. Este nivel se alcanza consignando y respetando los principios rectores de la ley, así como las medidas técnicas de seguridad y confidencialidad que correspondan a la categoría de datos de que se trate. Este nivel de protección viene a ser parte del contenido fundamental[20] de uno de los principios rectores de la ley, el consagrado en el artículo 11° como principio de nivel de protección adecuado para el flujo transfronterizo de datos personales.

3. Ámbito de aplicación

La Ley, de conformidad con lo establecido en su artículo 3°, es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. La Ley no se aplicará a los datos personales 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; así como a los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley en las materias relacionadas con la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito. Cabe precisar que de conformidad con el proyecto de reglamento de la Ley, se establecen especiales disposiciones sobre su ámbito de aplicación territorial.[21]

4. Tratamiento de datos personales

El tratamiento de datos personales es un concepto amplio consistente en 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 tratamiento mismo y su finalidad serán definidos por el titular del banco de datos, o por el responsable del tratamiento[22]. Lo que habilita el tratamiento de los datos personales es el consentimiento del titular de los mismos, el cual deberá ser previo, informado, expreso e inequívoco por disposición del artículo 13.5 de la Ley. Esta exige un consentimiento expreso, lo que la coloca en este punto como una norma de gran exigencia a la hora de la toma del consentimiento[23]. Las excepciones o limitaciones al consenti-

20 El principio de nivel de protección adecuado estaría respetado, según el artículo 11° referido, también cuando se garantice un nivel de protección equiparable a lo previsto por esta ley o por los estándares internacionales en la materia.

21 Ver artículo 5°. http://www.minjus.gob.pe/sites/default/files/documentos/portada/ley-datos-personales.pdf.

22 Según proyecto del reglamento prepublicado.

23 Sin llegar al nivel de exigencia contenida en el artículo 5.2 de la Ley de Costa Rica, que requiere un consentimiento expreso y escrito.

miento se encuentran reguladas en los diez incisos del artículo 14 de la Ley, que comprenden supuestos que podrían ser ampliados por el Reglamento. Para el caso de los datos sensibles, el consentimiento deberá ser, además, por escrito.

5. Principios rectores

El derecho a la protección de datos personales requiere, para su configuración, de la adopción de determinadas garantías y principios que son los que establecen las pautas a las que debe ajustarse todo tratamiento de datos personales desde el momento mismo de su recolección; la observación de los principios es garantía de un tratamiento adecuado de la información de la persona. En este sentido, la Ley peruana, con carácter enunciativo, consagra los siguientes ocho principios rectores[24]: de legalidad, de consentimiento, de finalidad, de proporcionalidad, de calidad, de seguridad, de disposición de recurso y de nivel de protección adecuado. El carácter enunciativo da margen para que el Reglamento pueda incluir otros principios que, por ejemplo, coadyuven a la mejor aplicación de la Ley; no obstante, el texto que se conoce no ha incorporado otros principios como pueden ser los de transparencia o de responsabilidad, considerados por diferentes legislaciones.[25] De conformidad con lo establecido en el artículo 12 de la Ley, el valor de los principios reside en que se constituyen en guías para la actuación de los titulares y encargados de los bancos de datos personales y, en general, de todos los que intervengan con relación a ellos, siendo que, además, servirán de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su Reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia.

6. Derechos del titular de datos personales

Los derechos que la Ley establece para el titular de los datos personales y que concretan los poderes de disposición y control sobre su información están regulados en los artículos 18 a 25: acceso del titular de datos personales; derecho de actualización, inclusión, rectificación y supresión; derecho a impedir el suministro; derecho de oposición; derecho al tratamiento objetivo; derecho a la tutela; y derecho a ser indemnizado.

El derecho a la tutela se ejercitará en caso de que el titular o el encargado del banco de datos personales deniegue al titular de dichos datos, total o parcialmente, el ejercicio de los derechos establecidos en la Ley, pudiendo recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación, así como al Poder Judicial para los efectos de la correspondiente acción de hábeas data. La resolución de la Autoridad Nacional de Protección de Datos Personales agota la vía administrativa y habilita la imposición de las sanciones administrativas previstas en el artículo 39 de la Ley. Contra

24 Ver artículos 4 al 12 de la ley.

25 Principio de transparencia: estándares internacionales aprobados por la Resolución de Madrid 2009. 10. página 12. Directrices de la ocde sobre protección de la privacidad y flujos transfronterizos de datos personales. Principio de responsabilidad: estándares internacionales aprobados por la Resolución de Madrid 2009. 11. página 13. Directrices de la ocde sobre protección de la privacidad y flujos transfronterizos de datos personales.

las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa. Los derechos contemplados en la Ley peruana incluyen los que, de manera general, la doctrina y legislación comparada[26] consideran, conceptualizando además otras medidas no tradicionalmente denominadas derechos[27].

. Flujo transfronterizo de datos personales

El flujo transfronterizo de datos personales solo puede realizarse desde el Perú hacia un país que mantenga niveles de protección adecuados conforme a la Ley. En el supuesto de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto por la Ley.[28]

Independientemente de los supuestos excepcionales en los que el flujo transfronterizo puede darse sin cumplir lo señalado en el párrafo precedente, ¿cómo la legislación peruana está previendo operativizar la transferencia internacional de datos hacia un país que no tenga niveles adecuados de protección equivalentes a los establecidos en la ley? El único parámetro propuesto hasta el momento está en el proyecto de reglamento publicado[29]. En dicho documento se señala que el emisor o exportador podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se establezcan, cuando menos, las mismas obligaciones a las que este se encuentra sujeto, así como a las condiciones en las que el titular consintió en el tratamiento de sus datos personales. Cualquiera sea el supuesto del flujo transfronterizo de datos personales, éste siempre se pondrá en conocimiento de la Autoridad Nacional de Protección de Datos. Asimismo, los titulares del banco de datos o responsables del tratamiento podrán solicitar la opinión de la Autoridad respecto a si el flujo transfronterizo de datos cumple con lo dispuesto por la Ley y su Reglamento.

8. Autorregulación

El tema de la autorregulación está normado en el artículo 31 de la Ley, cuando se da la facultad para que las entidades representativas de los titulares o encargados de bancos de datos personales de administración privada puedan 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 Ley. Con ello, se ratifica la naturaleza y el valor de estos instrumentos que encuentran su sentido pleno en ser un complemento a la legislación que expida el Estado, pues su sola existencia no es suficiente para la tutela adecuada

26 La ley mexicana contempla los derechos denominados ARCO: acceso, rectificación, cancelación y oposición, artículo 22; la ley española 15/1999, artículos 13 al 19: impugnación de valoraciones, acceso, rectificación y cancelación oposición, tutela e indemnización; la ley uruguaya, artículos 13 al 17: información frente a la recolección de datos, acceso, rectificación, actualización, inclusión o supresión, impugnación de valoraciones personales y derechos referentes a la comunicación de datos.

27 Ejemplo: derecho a impedir el suministro. Artículo 21.

28 Artículo 15.

29 Ver el proyecto de reglamento publicado en http://www.minjus.gob.pe/sites/default/files/documentos/portada/ley-datos-personales.pdf.

de un derecho fundamental. En el sentido señalado, la Autoridad Nacional de Protección de Datos Personales tiene asignada una función de promoción del uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales.[30]

9. Autoridad Nacional de Protección de Datos Personales

La Ley peruana, en su título VI, se ocupa de la Autoridad Nacional de Protección de Datos Personales. Esta Autoridad se encuentra dentro del ámbito de competencia del Ministerio de Justicia y Derechos Humanos a quien se le ha asignado como una de sus funciones específicas la del ejercicio de la misma[31].

Las funciones de la Autoridad Nacional de Protección de Datos Personales son de carácter administrativo, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras y se encuentran reguladas en veinte incisos del artículo 20 de la Ley; no obstante, dichas funciones no son señaladas de manera taxativa, pues de conformidad con lo que dispone el inciso 21 del mismo artículo, serán también sus funciones las demás que le asigne la Ley y el Reglamento. Asimismo, goza de potestades sancionadoras y coactivas, y tendrá a su cargo el Registro Nacional de Protección de Datos Personales.

El órgano de control o autoridad en la materia, por disposición del reciente Reglamento de organización de funciones del Ministerio[32], será la Dirección General de Protección de Datos Personales, que depende jerárquicamente del Viceministerio de Derechos Humanos y Acceso a la Justicia;[33] pues este tiene dentro de sus funciones la de supervisar a la Autoridad Nacional de Protección de Datos Personales. Los órganos de la dirección general de protección de datos personales están constituidos por las siguientes cuatro direcciones: registro nacional de protección de datos personales; supervisión y control; sanciones; normatividad y asistencia legal.

No encontramos en la Ley, en el proyecto de Reglamento ni en el Reglamento de organización y funciones del Ministerio, referencia explícita sobre el nivel de autonomía o de independencia técnica de la Autoridad; pero sí es explícito que ella será ejercida por una Dirección General, que si bien es cierto tiene competencia nacional, es un órgano de tercer nivel dependiente de un viceministerio. Como muestra de lo señalado podemos citar el Reglamento de organización y funciones del Ministerio de Justicia y Derechos Humanos que establece como última función específica de la Dirección General de Protección de Datos Personales "Otras funciones específicas que le asigne el Despacho Viceministerial de Derechos Humanos y Acceso a la Justicia o que le sean dadas por las normas respectivas", artículo 91, literal k). La designación de quien ostentará el cargo de Autoridad, será hecha por resolución Ministerial y con carácter de confian-

30 Artículo 33, inciso 13.

31 Mediante el reglamento de organización y funciones del Ministerio, aprobado por el Decreto Supremo Nº 011-2012-JUS.

32 *Ibidem*. Disponible en:

http://spij.minjus.gob.pe/CLP/contenidos.dll?f=templates&fn=defaultrofminjus.htm&vid=Ciclope:CLPdemo

33 Artículo 90 del reglamento de organización y funciones.

za, no estableciéndose un plazo de duración del mismo.

En América Latina, los temas de autonomía e independencia de los órganos de control han sido de constante discusión reflexiva, pues a diferencia de lo que sucede en Europa, en esta región debido a la estructura organizativa de las entidades estatales producto de la cultura organizacional política imperante, a aspectos presupuestales y al nivel de desarrollo de la democracia, no ha sido posible que los países que han creado autoridades en materia de protección de datos personales le hayan dado una independencia y autonomía equiparables a la que ostenta en Europa, por ejemplo, la Agencia Española de Protección de Datos. El Instituto Federal de Acceso a la Información Pública y Protección de Datos, de México, es el que evidencia una autoridad de control con el mayor nivel de autonomía en lo que al ámbito de Latinoamérica se refiere. El análisis de este tema es importante pues tiene relación directa con la efectividad del derecho. No es materia de este breve estudio, pero queda pendiente, el análisis de la efectividad de las autoridades de control en nuestros países[34]; salvo en Argentina, que ya tiene una historia que contar por los años recorridos, en los otros países con autoridades de control es muy pronto para hacer un estudio completo sobre dicho tópico. Esperamos que en el andar del ejercicio de este derecho, las autoridades se fortalezcan y estén a la altura de la tarea encomendada. Para el cumplimiento adecuado de sus funciones, las autoridades de control requieren contar con capacidad técnica, autonomía e independencia, lo que exige recursos materiales, humanos y económicos[35] mínimos, los cuales no siempre están garantizados, pues hay relación directa entre ello y el nivel de voluntad política al respecto. Creemos que, en el presente contexto, lo señalado es el principal reto que debe superar el Perú en materia de protección de datos personales.

34 Argentina. Se ocupa tanto en su Ley (artículo 29) como en su Reglamento (artículo 29) del denominado órgano de control. En dicho país, el órgano de control es la Dirección Nacional de Protección de Datos Personales, adscrita a la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos.

México. Se ocupa de la Autoridad de Protección de Datos en los "transitorios" del capítulo II de su Ley constitutiva del instituto en el siguiente artículo, "Artículo 33.- El instituto es un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades". El ifai, ente de control, ya existía como autoridad de transparencia y acceso a la información pública y en materia de protección de datos para el sector público.

Uruguay. Tanto en su Ley como en su norma reglamentaria se ocupan del tema de la autoridad de control. La Ley N° 18.331 le dedica el Capítulo VIII. Del Órgano de Control (unidad reguladora y de control de datos personales), dependencia desconcentrada de la Agencia de gobierno electrónico y Sociedad de la Información (agesic), en adelante la urcdp, la cual determina también la existencia de un consejo consultivo de la Unidad reguladora en protección de datos, los recursos y potestades sancionadoras de la Autoridad, así como los códigos de conducta. En su norma reglamentaria, aprobada por el Decreto N° 414/009, le dedica a la autoridad de control el capítulo IV, desarrollando los temas de la presidencia de la urcdp, de los cometidos del presidente de la misma, del Consejo Consultivo y de sus atribuciones y de su funcionamiento, entre otras. Cabe señalar que el reglamento uruguayo le dedica un título independiente, el título III, al régimen registral.

35 La ley de protección de datos personales, Ley N° 29773, publicada el 03 de julio de 2010, en su décima disposición complementaria final, dispone lo siguiente sobre el 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, sin demandar recursos adicionales al Tesoro Público." En igual línea, la Ley de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, Ley N° 29809, publicada el 11 de diciembre de 2011, establece en su primera disposición complementaria final, con el epígrafe Disposiciones para la implementación, lo siguiente. "Facúltese al Ministerio de Justicia y Derechos Humanos a emitir las disposiciones complementarias pertinentes, a efectos de la adecuación de la estructura orgánica y la implementación de la presente Ley. La aplicación de la presente norma se financia con cargo al presupuesto institucional del pliego Ministerio de Justicia y Derechos Humanos, sin demandar recursos adicionales al Tesoro público."

III. CONCLUSIONES

– América Latina sigue un ritmo propio en cuanto a la regulación del derecho a la protección de datos personales. Dicho ritmo se debe, entre otras razones, a que los legisladores en la mayoría de los países de esta región tienen un nivel medio-regular de conocimiento en la materia; a los episodios de interrupción constitucional en varios Estados y al hecho de que este tema no ha sido prioridad en la agenda política de las autoridades correspondientes.

– La regulación sobre la protección de datos personales en América Latina ha evolucionado significativamente en los años que van corridos en este nuevo milenio, traduciéndose esto, de manera particular, en la aprobación de leyes de carácter general con autoridades de control en cinco países: Argentina (2000), Uruguay (2008), México (2010), Perú (2011), Costa Rica (2011) y Nicaragua (2012).

– Dentro de las vías jurídicas que los países latinoamericanos han utilizado en la búsqueda de un equilibrio entre las transferencias internacionales de datos y un tratamiento adecuado de los mismos encontramos dos que se complementan: los instrumentos jurídicos supranacionales y la legislación interna.

– El sistema jurídico de protección de datos personales que está configurándose en América Latina se caracteriza por una situación de asimetría normativa; la existencia de una consideración política del tema a nivel regional; y la prevalencia inspiradora del modelo europeo, por lo menos en los países que ya cuentan con leyes generales y autoridades de control .

– La situación de asimetría normativa que caracteriza la legislación sobre protección de datos personales en América Latina, en atención a las opciones legislativas adoptadas por los diferentes Estados, nos muestra: Estados con ley de protección de datos personales de carácter general y con autoridad de control administrativa; un Estado con protección legislativa general pero sin autoridad de control administrativa; Estados con reconocimiento constitucional explícito del derecho a la protección de datos personales; Estados con reconocimiento constitucional explícito del recurso del hábeas data; Estados con reconocimiento constitucional explícito del derecho a la intimidad y a la privacidad; y Estados con legislación sectorial o vertical dispersa sobre protección de datos personales.

– En atención a la naturaleza de los diversos medios utilizados para el tratamiento de los datos personales y a la necesidad de las transferencias internacionales de los mismos, se hace necesario que los desarrollos normativos se den de manera armónica y a través de políticas de largo alcance, que posibiliten seguir avanzando hacia soluciones coordinadas en la materia.

EL CASO DE PERÚ

– Con la Ley N° 29733, el derecho fundamental a la protección de datos personales es desarrollado legislativamente y se crea una autoridad de control que se suma a la tutela jurisdiccional del mismo, existente en el hábeas data, pero ahora desde el ámbito administrativo.

– El legislador peruano ha optado por circunscribir al ámbito de protección de la Ley a la persona naturales, excluyendo a las personas jurídicas o morales.

– La Ley peruana, con carácter enunciativo, consagra ocho principios rectores: de legalidad, de consentimiento, de finalidad, de proporcionalidad, de calidad, de seguridad, de disposición de recurso y de nivel de protección adecuado.

– La Ley peruana consagra ocho derechos del titular de los datos personales: información; acceso; actualización, inclusión, rectificación y supresión; impedir el suministro; oposición; tratamiento objetivo; derecho a la tutela; y derecho a ser indemnizado.

– La Autoridad Nacional de Protección de Datos Personales se encuentra dentro del ámbito de competencia del Ministerio de Justicia y Derechos Humanos a quien se le ha asignado como una de sus funciones específicas la del ejercicio de la misma. El órgano de control peruano, o autoridad en la materia, será ejercido por la Dirección General de Protección de Datos Personales, órgano de línea del Viceministerio de Derechos Humanos y Acceso a la Justicia de quien depende jerárquicamente.

– Para el cumplimiento adecuado de sus funciones, las autoridades de control requieren contar con capacidad técnica y niveles adecuados de autonomía e independencia, lo que exige recursos materiales, humanos y económicos, los cuales no siempre están garantizados. En el contexto actual, el señalado es el principal reto que debe superar el Perú en materia de protección de datos personales.

Bibliografía

Constituciones políticas de los Estados de América Latina.

Directrices para la armonización de la protección de datos en la comunidad Iberoamericana de Protección de Datos. 2007. Red Iberoamericana de Protección de Datos.

Leyes:

Argentina. Ley N° 25326, Ley de protección de los datos personales. 2000.

Costa Rica. Ley de protección de la persona frente al tratamiento de sus datos personales N° 8969. 2011.

México. Ley federal de protección de datos personales en posesión de los particulares. 2010.

Nicaragua. Ley de protección de datos personales, Ley N° 787. 2012.

Perú:

Decreto Supremo Nº 011-2012-JUS. Reglamento de organización y funciones del Ministerio de Justicia y Derechos Humanos.

Ley de protección de datos personales, Ley N° 29733. 2011.

Ley N° 2786. Ley de transparencia y acceso a la información pública. 2002.

Ley Nº 28237. Código Procesal Constitucional. 2004.

Zamudio Salinas, M. de L., "Perú: La protección de datos personales". En *Lumen*, revista de la Facultad de Derecho de la Universidad del Sagrado Corazón. N° 7, enero a diciembre del 2010, Lima. 2010. pp. 127-135.

Tratados sobre materias de derechos humanos y economía.