EL ACTUAL DERECHO DE LA PROTECCIÓN DE DATOS EN AMÉRICA Y EUROPA

Marcelo BAUZÁ REILLY

SUMARIO: I. *Control social, democracia y privacidad*. II. *Un nuevo derecho, un nuevo peldaño*. III. *El derecho comparado*. IV. *Algunas conclusiones*.

I. CONTROL SOCIAL, DEMOCRACIA Y PRIVACIDAD

1. *Elementos fundacionales para un nuevo derecho*[1]

El presente análisis no pretende otra cosa que aportar una visión reflexiva, sinóptica y actual de un derecho fundamental en permanente evolución, cuyo reconocimiento y adecuada regulación normativa siguen abriéndose camino en la región latinoamericana, a través de la confluencia de modelos jurídicos reconocibles y vigentes (Europa y Latinoamérica). Estos modelos presentan el particularismo actual, desde no más de cuatro o cinco años a la fecha, de estar intentando afirmar su intensa sinergia y

[1] Además de las normas europeas comunitarias fundacionales de esta nueva concepción que luego reseñaremos (Carta de Derechos Fundamentales y Constitución de Europa), existen también piezas de jurisprudencia remarcables al respecto, como son la Sentencia del Tribunal Constitucional Federal alemán del 15 de diciembre de 1983, y la sentencia 292/2000 del 30 de noviembre de 2000 del Tribunal Constitucional español, que anuncian la emergencia de un "derecho fundamental a la protección de datos de carácter personal", independiente del derecho de intimidad, al que abraza pero al que también supera en varias facetas. El autor se ha extendido sobre las peculiares características y el devenir actual de este "movimiento de confluencias jurídicas" entre Europa y Latinoamérica, en su contribución al *Libro de homenaje a Mario Losano*, Montevideo, Dyckinson, 2006, a la fecha del presente en prensa) bajo el título "La protección jurídica de los datos personales en Uruguay a través de la Ley núm. 17.838".

relacionamiento, conforme pautas del mundo moderno y globalizado que tanto requiere de estos esfuerzos integradores. Nuestro análisis pondrá énfasis en aquellas notas que aparecen con mayor realce general, en particular para nuestra región.

En un rápido y básico enfoque del actual régimen jurídico de la "protección de datos personales" en el derecho comparado, encontramos el asiento de este régimen en tres nociones sociojurídicas fundamentales:

- La noción de *control social*, merced a la cual las conductas humanas trascendentes a la esfera social requieren de un control externo a quienes las ejercitan, so pena de ingresar en el conflicto o en la utopía anarquista.
- La noción de *democracia*, en tanto sistema de vida y gobierno de las sociedades contemporáneas que cumple y respeta principios básicos de convivencia tales como la libertad, igualdad, solidaridad, etcétera.[2]
- La noción de *privacidad*, que supone un ámbito de acciones e informaciones de la persona ajeno al escrutinio público.

En las sociedades actuales, estas tres nociones (valores) se encuentran en permanente tensión y construyendo de modo incesante su punto de equilibrio. Por lo tanto, la protección de datos personales, como institución jurídica moderna, ha experimentado ella misma las dinámicas y los reequilibrios que le imponen sus cimientos, en un devenir histórico de poco más de treinta años a la fecha que ha experimentado la institución.

Actualmente puede afirmarse con claridad que existen unos puntos de partida insoslayables que explican el origen y evolución de este derecho hoy reconocido como fundamental, y que son los siguientes:

- Las implicancias profundas de la informática y las comunicaciones electrónicas respecto de las garantías fundamentales.
- La preservación del ideal democrático.
- Un drama de época como es el de las relaciones entre las libertades individuales y las intervenciones del Estado.

[2] Rodotà, Stefano, "Democracia y protección de datos", *Cuadernos de Derecho Público*, Madrid, INAP, núms. 19-20, mayo-diciembre de 2003.

- La lógica totalitaria (el ciudadano que esconde algo es un enemigo del pueblo) enfrentada a la lógica democrática (los Estados deben tutelar la privacidad como derecho de toda persona).
- El rechazo a la idea del llamado "hombre de cristal".[3]
- La aceptación en cualquier plano, de medidas de recorte limitado y garantista de ciertos derechos y libertades, en función del bien público y la propia contribución a la democracia.

2. *Democracia y publicidad*

La democracia no es sólo "gobierno del pueblo" sino también "gobierno en público".[4]

A partir de este sagaz recordatorio, se constatan dos consecuencias ineludibles.

Por un lado, aflora en toda su magnitud el principio de transparencia de la vida pública, connatural a cualquier proceso democrático.

Por otro lado, existe igualmente un juego de tensiones entre el principio de transparencia y el principio de privacidad, donde a veces cede uno y otras veces cede el otro, en función de los postulados en juego.

Este tipo de razonamientos no resulta baladí en términos jurídicos, en particular respecto a la institución jurídica abordada. Por ejemplo: cuando un individuo decide libérrimamente ubicar sus acciones y conducta en la esfera pública (políticos, artistas, etcétera), la decisión que toma no es impermeable a ciertas consecuencias sociales. Por el contrario, ese mismo individuo atraerá hacia la esfera de su consentida publicidad, una parte mayor de datos privados que el común de los mortales.

Existen algo así como vasos comunicantes en función de los intereses y escenarios donde se mueven las personas. El "nivel" de estos vasos au-

[3] Metáfora utilizada por la jurisprudencia alemana en el célebre *leading case* fundacional de la "autodeterminación informativa", es decir la Sentencia del 15 de diciembre de 1983 del Tribunal Constitucional Federal sobre la Ley del Censo de Población. El autor escuchó por primera vez esta expresión, y posiblemente también hizo su primer contacto de alta calidad académica con la temática en juego, gracias a la contribución que Antonio-Enrique Pérez Luño tuviera la gentileza de enviar al primer evento académico de derecho informático realizado en Uruguay, contribución que expusimos verbalmente en su nombre y está publicada en los anales respectivos: "Informática y derechos fundamentales", *Primeras Jornadas Nacionales de Derecho Informático*, Montevideo 1987, pp. 119-135.

[4] Rodotà, Stefano, *op. cit.*, nota 2.

menta o disminuye según sea el tipo de escenario e intereses elegido por la persona para desenvolverse como tal.

Sin embargo, todo este planteo sigue estando lejos de la supuesta obligación (ni siquiera de esta clase de individuos más "expuestos"), en cuanto a tener que sufrir el imperativo de exhibir totalmente su esfera privada.

3. *Información y sociedad*

La vida social se ha convertido en un complejo y continuo flujo de datos, a merced del poder electrónico. Este fenómeno social de por sí evolutivo en sentido *in crescendo*, ha realzado el rol de la institución jurídica "protección de datos", como garantía igualmente dinámica que pasa a ubicarse en el centro mismo de cualquier sistema político-institucional que mantenga en alto las promesas y designios de la democracia.

Cada Estado, cada pueblo, tienen necesidad de construir los lindes y los mejores andariveles, para una organización y funcionamiento acordes con esta nueva realidad.

El actual "derecho fundamental de la protección de datos" es el instrumento jurídico preciso y refinado, que un buen número de países y regiones se viene dando para cumplir con este objetivo y acomodo a las nuevas realidades.

En palabras del director de la Agencia de Protección de Datos española, de lo que se trata es de lograr "la normalización de una auténtica cultura de la protección de datos personales".[5] A nosotros también nos resultan caras y dignas de insistencia este tipo de reflexiones, alejadas de la fría dogmática jurídica pero de vuelco tan necesario en el escenario político y social, a la hora de instaurar nuevas reglamentaciones jurídicas.[6]

[5] Piñar, José Luis, Diario de Sesiones del Congreso de Diputados (Comisiones, Constitucional) del 28 de septiembre de 2005, *https://www.agpd.es/upload/Conferencias/Comparecencia_Director_congreso.pdf.*

[6] Al respecto transcribimos dos intervenciones, ambas pronunciadas por el autor y contenidas en las actas de un Coloquio especializado celebrado hace un tiempo en Montevideo: Al comienzo del coloquio señalé que "No puedo terminar esta presentación sin dejar de señalar lo que espero resulte una constatación y un sentimiento a cambiar en nuestro país, Uruguay. Lo digo sin ambages: No tenemos una cultura ciudadana y militante en materia de protección de datos, algo que los europeos pienso que sí la tienen y actúan en consecuencia". A la terminación del mismo coloquio, y como corolario de la experiencia personal vivida en esa oportunidad al contacto con expertos nacionales y

II. Un nuevo derecho, un nuevo peldaño

1. *El momento actual*

Han transcurrido más de 35 años del dictado de las primeras leyes de protección de datos norteamericanas y europeas. Es un dato de la realidad jurídica que revela cuán importante y consistente es esta institución, poniendo de manifiesto la importancia de conocer la instancia actual de este dinámico proceso normativo, a través de sus ejemplos más relevantes.

Entendemos que son estos hitos actuales los que están señalando el derrotero más perfeccionado, como corolario natural de una histórica cosecha de experiencia que contienen este tipo de procesos evolutivos.

El artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea consagra el "derecho a la protección de datos de carácter personal" en términos autónomos al "derecho a la vida privada y familiar" (artículo 7 de la misma Carta), ambos enmarcados —junto a otros— en el "derecho a la dignidad humana" sobre cuyas especies se extiende todo el capítulo I de este moderno texto normativo.

Simultáneo a su declaración, se consagran a texto expreso algunas notas fundamentales (principios) de este derecho, como son el tratamiento leal, específico, consentido o legitimado por ley, de los datos personales. Igualmente por lo que refiere al derecho de acceso y rectificación, así como el principio de control del régimen por autoridad independiente.

Otro texto clave para entender el rumbo actual de la institución, es el artículo 51 de la Constitución de la Unión Europea. De tono más general

extranjeros, me extendí en mayores consideraciones de las que solamente cito la siguiente: "Una falta de encarnadura en virtud de la cual, sospechamos, pagan tributo incluso nuestros legisladores. Esto se constata cuando a lo largo de los últimos años nuestros legisladores se han ocupado del asunto, pero lo han tomado en una forma segmental, asumiendo quizás las puntas más dramáticas, o más mediáticas incluso, de este tema, cuando en realidad el tema de los datos personales es un tema más vasto y organizado, que hay que regularlo —si es que se va a regular— de una manera mucho más general y orgánica". La primera cita corresponde al capítulo de "Introducción" al Coloquio "La protección de datos personales" realizado en Montevideo del 14 al 16 de mayo de 2003 (Instituto Goethe y otros). La segunda al capítulo "Conclusiones (2)" del mismo Coloquio. Las Actas de este interesante encuentro de academia, instituciones públicas y privadas, y sectores sociales involucrados, fueron recogidas en un volumen de varios autores, *Seguridad, privacidad, confidencialidad. El desafío de la protección de datos personales*, Montevideo, Trilce, 2004.

que el texto enunciado, igualmente exalta la protección de datos de carácter personal como derecho autónomo y establece el principio de legalidad (nacional y europea) en la materia, obligatorio para los Estados miembros "en el ejercicio de las actividades comprendidas en el ámbito de aplicación del derecho de la Unión, y sobre la circulación de estos datos". Consagra asimismo el principio de control a cargo de autoridades independientes.

2. *La PDP entendida como nuevo derecho fundamental*

Debe insistirse acerca de un punto clave de entendimiento: la protección de datos personales ha alcanzado en los últimos tiempos el estadio de nuevo derecho fundamental autónomo.

Resulta importante destacar las notas esenciales de este nuevo derecho, tal como ha venido a configurarse a partir de su peculiar proceso evolutivo.

Es *independiente* de su pariente más cercano, que no es otro que el respeto de la vida privada y familiar sin perjuicio de que también se lo ha vinculado (de modo más o menos diverso a estas nociones) con el derecho de intimidad. En los más modernos y actuales regímenes, la protección de datos personales ya no está solapada o confundida con ninguno de estos derechos.

Es *multifacético* porque contiene numerosos principios generales, se aplica sobre distintos momentos del dato personal (captura, tratamiento, etcétera), e incluye diversas vías de tutela.

Está *asegurado por instituciones oficiales especiales e independientes*, con poderes de control e intervención.

Es en esencia *libertario* y *solidario*, en el sentido de contribuir decisivamente al compromiso del individuo con sus pares en sociedad (sutil propiedad o enfoque, mucho menos conocido que divulgada vinculación con el derecho de intimidad, y que configura la columna vertebral de fundamento y entendimiento de la Sentencia del Tribunal Constitucional alemán del 15 de diciembre de 1983).

3. *Factores influyentes en la emergencia y desarrollo de la PDP*

Una visión sinóptica y reflexiva como la prometida en nuestro título inicial, no puede prescindir de pasar revista a algunas de las cuestiones y necesidades sociojurídicas que están presentes y explican la evolución experimentada por este régimen jurídico tan particular.

Hay que ser conscientes que todo es el fruto, en última instancia, de una larga evolución del concepto de privacidad. Es parte de aquel concepto original norteamericano del "derecho a ser dejado solo". Y se llega en periplo histórico al reconocimiento de la necesidad social de la externalización del dato personal, pero sometido a contra-poderes de legalidad, autodeterminación y control.

Llegamos así a una nueva manera de entender la protección de datos personales, que bien puede ubicarse a través de las nociones antes vistas (democracia, publicidad, etcétera) en términos radicales de "derecho de acceso" y "autodeterminación", lo que paradójicamente favorece la apertura —de un modo u otro, con las prevenciones y reglas adecuados— de todo aquello definido *a priori* (muchas veces irracionalmente) como secreto.

Hay una saludable apuesta subyacente (y no tanto) a la caída definitiva de la "cultura del secretismo" de los archivos públicos y privados y a poner todas las baterías jurídicas al servicio del aumento y proliferación de posibilidades para hacer efectivo el principio de transparencia del devenir social en todos los terrenos (gobierno, empresas, instituciones en general).

Otra realidad insoslayable e influyente viene dada por la circulación transfronteriza de datos personales. Tan importante como que está en la base de la regulación comunitaria europea.

En un plano más global de las relaciones internacionales, y atendiendo a la endémica falta de tratados, se rescata la necesidad de intervenciones jurídicas nacionales concertadas. En la medida que haya consensos acerca de los principios fundamentales del nuevo régimen, disminuirá la necesidad de regular la "exportación/importación" del dato personal.

Teniendo en cuenta la movilidad actual (personas, mercancías, actividades comerciales y científicas, información) la existencia de prácticas compartidas en la materia contribuye a procrear un tráfico más fluido, evitando asimetrías.

Existe igualmente la necesidad de reafirmar el principio favorable a la "libre circulación de la información", equilibrándolo con el régimen de protección de los datos personales que supone restricciones a su colecta, tratamiento y difusión.

4. *Protección de datos en Internet*

Una forma de bajar las construcciones teóricas a las constricciones de la realidad, al menos para la materia en examen, es traerla a uno de los esce-

narios más extendidos y necesitados de marcos regulatorios, como es el de las redes telemáticas. El uso expandido de éstas determina con carácter inexorable que los datos personales circulen, se acumulen y se traten en su seno, con todos los desafíos de regulación y control que ello implica.

En nuestro enfoque de tono prospectivo, nos limitaremos a señalar la presencia irresistible de este factor (uso expandido de redes como escenario real y frecuente del dato personal), que lleva a considerar como *desideratum* el dictado de políticas y derechos acerca tanto de datos personales y comercio electrónico, como de datos personales y gobierno electrónico.

La necesidad en constante incremento de compartir información, pero asimismo de hacerlo con resguardo y responsabilidad (datos sensibles), provoca en ambos ámbitos (gobierno y comercio electrónicos) sinergias técnicas y sociales en torno a la interoperabilidad y apertura de archivos digitales, que deben resolverse con arreglo a este nuevo derecho fundamental. La preservación del dato íntimo o confidencial así como seguridades de diversa índole pero siempre conectadas (física, lógica y jurídica) de tales datos, son parte inescindible de cualquier proyecto o emprendimiento concreto en estos campos.

Por esta senda reflexiva se llega fácilmente a conclusiones tales como que el régimen de protección jurídica de los datos personales forma parte de las condiciones de viabilidad de cualesquiera de estos procesos (comercio y gobierno electrónicos). Y otra conclusión importante es que, entendido el régimen de protección de datos personales como "nuevo derecho fundamental", se adapta mucho mejor a todos estos procesos.

5. *El nuevo modelo asociado a mayor democracia y bienestar*

El análisis hasta aquí practicado provoca como conclusión primera la presencia en el escenario social y jurídico más evolucionado de un cambio profundo en el papel de la privacidad. Papel que, sin perder parte de su fisonomía original, se completa con otro tipo de ideas o paradigmas, como son la lucha contra la discriminación y la elección libre de opciones de vida.

Se opera de esta manera una mutación revolucionaria: el reconocimiento a toda persona de un poder permanente de control sobre sus propios datos donde quiera se encuentren esos datos, incluso si estuvieren en archivos de naturaleza preservada (servicios secretos), en el entendido que siempre existirán formas y mecanismos para dar satisfacción a este nuevo

valor sin desmedro de sigilos y secretos de reserva legal (a través, por ejemplo, del llamado acceso "indirecto").

Una síntesis magistral acerca de este nuevo modelo, digna del experto de primera clase que la sostiene, es aquélla que pone de relieve que, desde el momento que la "protección de datos" garantiza la capacidad de la persona para comunicarse y participar socialmente, su previsión y su régimen jurídico acordes pasan a ser elementos determinantes de la existencia y función de una sociedad democrática.[7]

En esencia éste es el nuevo modelo. Un modelo indisolublemente asociado a un concepto de democracia ajustada o entendida conforme los tiempos que corren, que no es otra cosa que seguir apostando a la racionalidad humana y solidaria en tiempos de globalización electrónica.

III. El derecho comparado

1. *Derecho europeo. Estadio actual*

En materia de protección de datos personales Europa presenta una situación que no dudamos en calificar de robustez y tradición jurídica.

Por un lado el derecho comunitario europeo cuenta con tres tratados, dos de ellos regionales[8] y uno sectorial.[9] De su parte son 32 los países que

[7] Simitis, Spiros, "Los fundamentos políticos y sociales de la protección de datos", que recoge las palabras de este pionero en total vigencia, pronunciadas en la Conferencia de Primavera de las Autoridades Europeas de Protección de Datos, Cracovia 25-26 de abril de 2005, publicado en la revista digital *datospersonales.org*, Madrid, APD, núm. 17, 29 de septiembre de 2005, *http://www.madrid.org/comun/datospersonales/0,3126,457237_457444_127535941_12411296_12403934,00.html*.

[8] Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, celebrado en Estrasburgo el 28 de enero de 1981 (conocido vulgarmente como Convenio de Estrasburgo en la materia); 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.

[9] Directiva 2002/58/CE, del Parlamento Europeo y del Consejo del 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Si bien no puede decirse que la problemática en juego en este sector con respecto a "datos personales" se haya escindido de su tronco común, en cambio es indiscutible que ha adquirido sesgos de necesario tratamiento puntual y diferenciado. Así lo acredita la prolífica doctrina dedicada al tema, por ejemplo Roca Junyent, Miquel y Torralba Mendiola, Elisa, "Derecho a la intimidad: el secreto y de las

cuentan con estatutos jurídicos y autoridades de control nacionales en la materia, incluyendo curiosos ejemplos como Guernesey, Jersey, Isla de Mann.

Entre los más destacados ejemplos está España con su Ley Orgánica 15/1999, Francia con su Ley 78-17 (modificada en 2004), Italia con el Decreto legislativo 196/2003. Países como España también insertan competencias en la materia en sus circunscripciones territoriales autónomas.[10]

Existe una intensa actividad comunitaria regular alrededor de este régimen. Entre lo más destacado la que se desarrolla por medio del Supervisor Europeo de Protección de Datos, los acuerdos de Schengen, Europol y Eurojust, el Grupo artículo 29, las conferencias de Primavera (europea) e Internacional de Autoridades de Protección de Datos, y el Grupo de Telecomunicaciones de Berlín.

Europa ha evolucionado así en función de un decidido intervencionismo legislativo, al contrario de Estados Unidos, y hasta cierto punto América Latina (que comienza a completar en los últimos años su estrategia principista y constitucionalista con estatutos legales y reglamentarios).

Todos estos regímenes, por una vía u otra, con matices semánticos que no alteran el norte evolutivo común, prevén el reconocimiento de directrices (principios) de necesario respeto:

- Recopilación y procesamiento justo y legítimo.
- Exactitud.
- Especificación y limitación de objetivos.
- Proporcionalidad.
- Transparencia.
- Participación individual (derecho de acceso).

comunicaciones" y Asís Roig, Agustín E. de, "Protección de datos y derecho de las telecomunicaciones", ambas publicadas en un volumen colectivo sobre *Régimen jurídico de Internet*, Madrid, La Ley, 2002, pp. 181-199 y 201-228 respectivamente.

[10] La Agencia de Protección de Datos de la Comunidad de Madrid tiene competencias propias en torno a ficheros de titularidad pública creados o gestionados por la Comunidad Autónoma de Madrid, entes que integran la administración local de su ámbito territorial, universidades públicas y corporaciones de derecho público representativas de intereses económicos y profesionales de la misma, *www.madrid.org/apdcm*. Su revista digital se ha erigido en un referente especializado importante, por la abundancia de informaciones de actualidad, legislación, doctrina y jurisprudencia que contiene *www.datospersonales.org*. De tenores similares la Agencia Catalana de Protección de Datos, *www.apdcat.net* y la Agencia Vasca de Protección de Datos, *www.avpd.euskadi.net*.

- No discriminación.
- Seguridad.
- Responsabilidad.
- Supervisión independiente y sanción legal.
- Nivel adecuado de protección (flujos transfronterizos).

En igualmente rápida reseña, podemos señalar que las competencias de una autoridad de control europea (modelo español) son las siguientes:

- Publicidad de tratamientos y ficheros.
- Inspección y sanción (educación y prevención).
- Atención al público (información, recepción de peticiones y denuncias).
- Cooperación en la elaboración y aplicación de normas y códigos-tipo.
- Autorización de transferencias internacionales de datos.
- Participación en foros académicos y cursos formativos.
- Relaciones y cooperación internacionales.

2. *Derecho latinoamericano. Estadio actual*

América Latina presenta un panorama regulatorio en la materia que cabe calificar como fragmentado y todavía débil, no obstante algunos progresos significativos.

La inexistencia de una unidad regional que reagrupe y cohesione las realidades nacionales de por sí diversas, conspira contra avances mayores o más rápidos que los observables. Una visión realista y completa de factores no puede dejar a un lado en la explicación también "el bajo nivel de desarrollo tecnológico en la década de los años setenta, y los gobiernos totalitarios que reinaban a principios de la década del ochenta".[11]

Existen regulaciones que cabría clasificar como "constitucionales" y "legales" por una parte, como "generales" y "sectoriales" por la otra. Mucho énfasis en derecho esencial, principista y garantista; poco énfasis en el derecho sustantivo, especializado y articulador al detalle. Completa el panorama latinoamericano el prestigio ascendente de la acción de *habeas data*.

[11] Dubié, Pedro, "¿Quo Vadis Iberoamérica fija un rumbo en protección de datos", revista digital, *datospersonales.org*, Madrid, APD, núm. 17 del 29 de septiembre de 2005, *http://www.madrid.org/comun/datospersonales/0,3126,457237_457444_127535941_12367707_12403934,00.html.*

Existe igualmente un proceso de cooperación Europa-Latinoamérica íntimamente relacionado con el estándar adoptado por la primera en materia de transferencia de datos personales a terceros países (lo que tradicionalmente se conoce como *flujo o movimiento transfronterizo de datos*), que actualmente regula el artículo 25 de la Directiva núm. 46 del 24 de octubre de 1995 (en especial su apartado 6), y se completa con criterios evaluatorios más detallados provenientes del llamado "Grupo Artículo 29" (por estar previsto en dicho artículo de la Directiva núm. 46).

En Argentina el artículo 43 constitucional, párrafo 3, consagra la acción de *habeas data* a favor de toda persona, para tomar conocimiento de sus datos y finalidad, que consten en registros o bancos de datos públicos o privados destinados a proveer informes, y en caso de falsedad o discriminación exigir supresión, rectificación, confidencialidad, actualización. Por su parte la Ley 25.326 de protección de los datos personales de 2000, reglamentada en 2001, es uno de los ejemplos a seguir como ley general. Argentina es el único país latinoamericano que goza del *ut-supra* referido estatus de "nivel de protección adecuado" con respecto a los datos transmitidos por la Comunidad Europea, por decisión de la Comisión.[12] La autoridad de control es la Dirección Nacional de Protección de Datos Personales emplazada en la Secretaría de Justicia del gobierno nacional.

En cambio Brasil no tiene norma general. Su régimen en la materia proviene de la Constitución federal que prevé el *habeas data* (artículo 5, LXXII), la protección a la intimidad y la vida privada (artículo 5, X) y la inviolabilidad de las comunicaciones donde se sitúan los datos (artículo 5, XII). Igualmente existe una reglamentación del *habeas data* a través de la Ley 9507/97. Varias leyes completan el abanico regulatorio de este país en algunos sectores altamente vinculados a la protección de datos personales, como son los bancos de datos y relaciones de consumo, la interceptación telefónica y grabación ambiental, y el levantamiento de sigilo bancario en delitos graves.

El caso de Chile nos coloca ante un reiterado ejemplo donde su Constitución, en el artículo 19-4, asegura a todas las personas el respeto y protección a la vida privada y pública, y a la honra de la persona y de su familia. La Ley 19.628 "sobre protección de la vida privada" de 1999 (modificada por la Ley 19.812 de 2002) es una ley general, si bien excluye los trata-

[12] Decisión C (2003) 1731 de 30 de junio de 2003, dictada por la Unión Europea.

mientos que se realicen por ejercicio de las libertades de opinión e información. Existen numerosas normas sectoriales: no discriminación laboral, correo electrónico laboral, prohibición de comunicar datos sobre obligaciones extinguidas o de monto inferior a cierta suma, eliminación de cierto tipo de datos en comunicaciones de información financiera, reserva de datos sanitarios.

El marco general en México lo da igualmente la Constitución federal, artículo 16, que establece el derecho de privacidad: nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones; regula la práctica de cateos, visitas domiciliarias, exhibición de documentos y papeles personales, y violación de correspondencia. La Ley Federal de Transparencia y Acceso a la Información Pública de 2002 posee un capítulo dedicado a la protección de datos personales, donde se establece el acceso y corrección de la información de carácter personal. Existen igualmente normas sectoriales: ley de salud pública (acceso a expedientes médicos); ley de imprenta (ataques a vida privada); ley de información estadística y geografía (prohibición de publicar en una sola estadística datos de una sola persona física o moral, y exigencia de desagregación); ley de sociedades de información crediticia (datos personales del buró de créditos y bancos).

En Panamá no hay preceptos constitucionales relacionados, a no ser sobre la inviolabilidad de correspondencia, papeles privados, y comunicaciones telefónicas. Tampoco hay norma general, pero en cambio se cuenta con normas sectoriales: Ley 6 de 22 de enero de 2002 sobre transparencia en la gestión pública y acción de *habeas data* ante entidades públicas o privadas que, por concesión, brinden servicios públicos; Ley 25 de 23 de mayo de 2002 que regula el servicio de información sobre solvencia de crédito.

Referido a Paraguay el artículo 33 de su Constitución consagra la habitual fórmula del "inviolable" respecto de la intimidad personal y familiar, y el respeto de la vida privada, extendiendo la garantía a la "protección de la intimidad, de la dignidad y de la imagen privada de las personas". Por su parte, el artículo 135 del mismo cuerpo estatuye el *habeas data* en planos sustantivos (derecho de acceso a la información y datos sobre la persona y sus bienes en registros oficiales o privados de carácter público, tanto como derecho a conocer el uso y finalidad de los mismos), como igualmente en el terreno procesal consagrando una acción específica ante magistrado competente, para la actualización, rectificación o destrucción de dichos registros, según las circunstancias. La normativa constitucional se completa con la Ley 1.682 de 16 de enero de 2001 (modificada parcialmente por la

Ley 1.969 de 2 de septiembre de 2002), que regula todas las etapas de vida del dato personal (recolección, almacenamiento, etcétera) destinado a dar informes, cuando los mismos fueran erróneos o afectaren ilegítimamente los derechos del titular.

Otro caso donde la balanza se inclina de momento hacia las normas constitucionales, es Ecuador. La Constitución de este país, en su artículo 23-8 garantiza intimidad personal y familiar. El artículo 23-21 del mismo cuerpo prohíbe utilizar información personal de terceros referente a creencias religiosas, filiación política, salud y vida sexual. Y el artículo 94 sobre *habeas data* establece el derecho de acceso a documentos, bancos de datos e informes sobre sí mismo o sus bienes, en entidades públicas o privadas, así como a conocer uso y propósitos; derecho de solicitar actualización, rectificación, eliminación o anulación; derecho a ser indemnizado si la falta de atención causare perjuicio. Preceptúa igualmente el dictado de un procedimiento legal especial para tener acceso a datos en archivos de defensa nacional. No existe norma legal general. La Ley de comercio electrónico, artículo 9, prohíbe la recopilación o cesión, etcétera, de datos personales. La Ley de Estadísticas y Censos prohíbe usar información para otros fines.

Para Bolivia se destaca la Constitución con su artículo 6, una de las escasas normas latinoamericanas de ese rango —si no la única— que reconoce la dignidad humana como derecho fundamental a respetar y proteger por el Estado. La carta magna de este país igualmente consagra en su artículo 23 la "acción de *Habeas Data*" en términos bastante precisos y modernos merecedores de destaque:

> I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de *Habeas Data* ante la Corte Superior del Distrito o ante cualquier juez de partido a elección suya.
> II. Si el tribunal o juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado.
> III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo.

IV. El recurso de *Habeas Data* no procederá para levantar el secreto en materia de prensa.
V. El recurso de *Habeas Data* se tramitará conforme al procedimiento establecido para el recurso de amparo constitucional previsto en el artículo 19 de esta Constitución. (Modificado por Ley 2410 del 8 de agosto de 2002).

Finalmente mencionaremos a Uruguay, donde la Constitución de la República no contiene normas expresas. No obstante ello, la presencia del derecho a la protección de los datos personales se infiere de un conjunto de artículos de la carta magna que consagran la llamada "estimativa jusnaturalista constitucional": artículos 7, 10, 28, 72, 332. La Ley 17.838 de 2004 ha abierto el camino de las regulaciones legales, si bien hubiera sido preferible una norma legislativa general en este punto, en vez de circunscribirse a la "protección de datos personales utilizados en informes comerciales y acción de *habeas data*". Otras normas habilitantes sectoriales son la Ley 16.736, artículo 694, sobre derecho de acceso frente a la administración; decretos 258/992 y 396/000 sobre datos sanitarios. En punto a datos de personas menores de edad, el Código de la Niñez y la Adolescencia (2004), artículos 218 y ss., crea el Sistema Nacional de Información sobre Niñez y Adolescencia a cargo del INAU, previendo un uso reservado y confidencial de los datos, y la destrucción de antecedentes judiciales y administrativos en conflicto con la ley al cumplir los 18 años de edad o el cese de la medida de seguridad sobre el menor.

3. *El incipiente movimiento iberoamericano de PDP*

En tiempos recientes los "Encuentros Iberoamericanos de Protección de Datos" y la "Red Iberoamericana de Protección de Datos"[13] han venido

[13] Creada bajo fuerte impulso de la Agencia Española de Protección de Datos en el II Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua, Guatemala (junio de 2003), en acuerdo de los 14 países iberoamericanos representados en dicha instancia. Se erige como foro integrador de numerosas realidades, públicas y privadas, que requieren de un hilo orientador destinado a producir avances en el reconocimiento y regulación de este derecho. El escenario mayor donde se dialogan y se plasman decisiones y documentos de la *Red Iberoamericana* son los Encuentros Iberoamericanos Anuales de Protección de Datos (EIPDs), de los cuales se llevan celebrados cuatro: El Escorial-España (2002), La Antigua-Guatemala (2003); Cartagena de Indias-Colombia (2004), Ciudad de México y en Huixquilucan, México (2005). Asimismo se han creado "Grupos de Trabajo" integrados por miembros de la Red, con el propósito de desplegar los proyec-

marcando un derrotero con pretensiones de difundir y estimular la aparición, encauce y vigencia de esta nueva institución jurídica en todos los países de la región, en función de postulados esenciales irrenunciables sin perjuicio de mecanismos y modalidades propios de cada país.

Desde otra perspectiva, enmarcada esta vez en uno de los encuentros cumbre periódicos de los últimos años que llevan a cabo los jefes de gobierno de la región, la "Declaración de Santa Cruz de la Sierra" contiene entre sus extensos compromisos el punto 45, directamente alusivo a la materia objeto de análisis y —más aún— legitimando los impulsos regionales derivados de la Red Iberoamericana:

> 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.[14]

IV. Algunas conclusiones

La "protección de datos personales" se ha convertido prácticamente en una rama jurídica en el derecho comparado,[15] y en ese sentido requiere constantes dosis de mayores previsiones normativas.

tos de ejecución resuelta en cada Encuentro, uno de los cuales ha venido trabajando desde el EIPDs de Cartagena de Indias (2004) sobre la viabilidad de creación de autoridades de control en el entorno latinoamericano.

[14] XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Declaración de Santa Cruz de la Sierra del 14 y 15 de noviembre de 2003.

[15] Así lo está viendo con claridad y fuerza la doctrina europea. Piñar Mañas, José Luis, actual director de la Agencia Española de Protección de Datos y catedrático de Derecho administrativo, nos dice al respecto: "En 2000 la situación experimenta un giro copernicano tanto en la Unión Europea como en España. Se abre una nueva etapa, en la que nos encontramos, que se basa en la consideración de la protección de datos de carácter personal como un verdadero derecho fundamental autónomo e independiente del derecho a la intimidad. Tan radical innovación deriva fundamentalmente de la Carta de los Derechos Fundamentales de la Unión Europea, proclamada en la Cumbre de Niza de 7 de diciembre de 2000, que, de forma lacónica pero tajante, dispone en su artículo 8, dentro del Capítulo relativo a las libertades, que toda persona tiene: '*Derecho a la protección de los datos de carácter personal que la conciernan*'." Ninguna referencia a la intimidad o privacidad; ninguna a la informática. Sí una previsión expresa, de suma importancia, al hecho de que "*el respeto de estas normas* [sobre protección de datos] *quedará sujeto al control de una*

En tal sentido creemos que la fuerza de la realidad ha terminado por sepultar el debate que pudo darse en el pasado reciente acerca de la eventual suficiencia de regímenes normativos de tipo genérico (constitucionalista) o principistas (constitucionalistas y analógico-legales) en los que, al menos nosotros, nunca creímos, de cara a presentar una "protección adecuada".[16] La necesidad acuciante de normas resulta evidente desde hace años en ciertas regiones como la latinoamericana, máxime si comparamos con el fuerte estado evolutivo del derecho europeo en la misma materia.

Refiriéndonos al derecho uruguayo, que puede resultar paradigmático de lo que sucede también en otros países de la región, y que es por fuerza el que más conocemos y apreciamos de cercano, no dudamos en advertir que queda aún mucho camino por recorrer a pesar del dictado de la Ley 17.838. Es de orden señalar que apenas comenzamos a advertir que estamos en presencia de una institución jurídica robusta, de dilatada vigencia y ejercicio en otras latitudes, y cuya experiencia en forma balbuciente comienza a ser aprovechada también en el medio vernáculo.[17] Se trata de una apreciación que no nos cansaremos de recordar: existe bastante desconocimiento entre nosotros sobre la institución jurídica mayor de derecho sustantivo dentro de la cual funciona un mecanismo más particular y garantista como es la "acción de *habeas data*, lo que contrasta con el desarrollo en otros países europeos y algunos latinoamericanos. Hay aquí, pues, un universo de conceptos jurídicos del que nuestra praxis jurídica figura alejada".[18]

autoridad independiente", "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*, Madrid, INAP, núm. 19-20, mayo-diciembre de 2002, pp. 45-90.

[16] Delpiazzo, Carlos "Conclusiones (1)", *op. cit*., nota 6.

[17] Muestra de ello puede ser la sentencia núm. 118/005 de 17 de octubre de 2005 dictada por el Juzgado Letrado de lo Contencioso Administrativo, que resuelve favorablemente una acción de *habeas data* entablada para tener acceso a informaciones de tipo gremial contenidas en el Sistema Nacional de Información del Ministerio de Salud Pública. Si bien el fallo descarta la aplicación de la Ley 17.838 por considerar que esta norma circunscribe su campo total de acción a los datos comerciales (posición que no compartimos), de todos modos fluye con evidencia un manejo de nociones que hasta no hace mucho nuestra jurisprudencia sencillamente ignoraba.

[18] Numerosos fallos nacionales dan testimonio de ello, resolviendo asuntos naturalmente pertenecientes a esta rama sin hacer la más mínima aplicación de nociones o principios de la misma. Entre otros pueden citarse: TAC 5 sentencia 52/97, LJU 13303 (negativa de legitimación de persona jurídica por daño moral, en juicio contra empresa proveedora de informes comerciales); TAC 2, sentencia 102/98, LJU 13591 (rechaza acción de amparo por comunicación parcialmente errónea de datos al no existir mala fe ni "ilegitimi-

Por tanto la comunidad jurídica uruguaya se encuentra ahora en mejor condición para echar mano a un conjunto profuso de postulados y previsiones de raigambre mayor, prácticamente ignoto antes del advenimiento de la Ley 17.838, si bien afincado en temáticas que venían siendo comentadas y tratadas desde hace algunos años a esta parte por una doctrina extremadamente puntual sobre el tema.

Hoy soplan nuevos vientos en materia de protección de datos personales entendida como derecho fundamental digno de una regulación precisa y unos controles sobre su cumplimiento, al igual que en muchos otros países del continente.

dad manifiesta"); J. L. Las Piedras, 4 sentencia 151/99, LJU 13887, con nota del doctor Alfredo Fernández Vicente (condena por daño moral a acreedor y empresa proveedora de informes comerciales, por inscripción de deuda menor en banco de datos, concomitante con negativa presunta del acreedor a ejecutar la deuda); TAC 5, sentencia 99/99, LJU 13888 (reconoce error de inscripción en registro de morosos, pero niega que ello implique daño moral reparable *per se* o sea sin necesidad de prueba); TAC 5, sentencia 30/03, LJU suma 129027 (admite irrogación de daño extramatrimonial por injusta categorización de morosidad).