LA TUTELA JUDICIAL Y ADMINISTRATIVA DEL DERECHO A LA PROTECCIÓN DE DATOS EN LA ARGENTINA

OSCAR RAÚL PUCCINELLI (ARGENTINA)
UNIVERSIDAD NACIONAL DE ROSARIO
PONTIFICIA UNIVERSIDAD CATÓLICA ARGENTINA
CEDDAL

1. INTRODUCCIÓN: LA PROTECCIÓN DE DATOS EN INDOIBEROAMÉRICA.

Partiendo de la idea de que cualquier derecho individual sin garantías termina convirtiéndose en una quimera, indica con acierto Estadella Yuste que el derecho a la protección de datos ha sido objeto de variadas regulaciones en el ámbito nacional e internacional, especialmente en estas modalidades: 1) Protección de carácter constitucional. 2) Protección de rango legal, a través de leyes nacionales de protección de datos, de carácter ómnibus o sectoriales. 3) Otras formas de protección derivadas de la práctica del sector público y privado, entre las que se encuentran: a) los códigos de conducta elaborados por el sector privado o público, y b) los contratos-acuerdo, que son los que reciben la aprobación de la autoridad nacional de protección de datos y son usados en las transferencias internacionales de datos. 4) Protección judicial y administrativa, a partir de las resoluciones dictadas por: a) tribunales constitucionales y ordinarios. b) autoridades nacionales de protección de datos, y c) la jurisprudencia internacional[1].

Es que el derecho a la protección de los datos personales, como cualquier derecho individual que esté desprovisto de garantías, por más carácter operativo que en la teoría ostente, es un derecho cuya vigencia depende en definitiva del mayor o menor grado de acatamiento espontáneo de la sociedad en general, o del nivel de exigibilidad que le reconozcan los restantes operadores jurídicos. Aun cuando reivindicamos la autonomía del nuevo derecho, no podemos menos que coincidir con Estadella Yuste y con Garzón en que "la cuestión de la protección de los datos personales no estriba tanto en añadir un nuevo derecho fundamental al repertorio de los ya conocidos, como en asegurar el disfrute efectivo del conjunto de tales derechos"[2].

Ahora bien: tratándose de un derecho de muy reciente factura –y cuanto más reciente es la aparición de un derecho, más frágil suele ser su posición–, es obvio que exige de mecanismos tutelares adecuados, lo que ordinariamente se establece a través de herramientas tanto genéricas (v.gr., las reglas constitucionales que reconocen el derecho a la protección de datos) como específicas (v.gr., las leyes sobre protección de datos que establecen las reglas para su tratamiento, o las reglas constitucionales y legales que incorporan el hábeas data como proceso constitucional destinado a tutelar el derecho a la protección de datos), que sean realmente eficaces para asegurar la mentada vigencia, que ya en buena parte se encuentra jaqueada por la existencia de un mercado informal potenciado por las herramientas telemáticas, el cual opera en algunas áreas (en especial, en el ciberespacio), casi sin controles.

Y entonces la efectivización del derecho a la protección de datos reclama el dictado de un marco adecuado de normas protectoras que, por un lado, establezca reglas claras para el tratamiento de datos que funcionen como garantías tanto para los tratantes de datos personales (lo hagan o no profesionalmente), como para los registrados en los sistemas de información de aquéllos, y, por el otro, permita una rápida reacción estatal ante el accionar ilegítimo, el que debe desarrollarse en dos dimensiones de control: la judicial y la administrativa.

En este sentido, en el ámbito internacional global, entre las directrices para la reglamentación de los ficheros computadorizados de datos personales (Resolución de la

[1] En cuanto a la jurisprudencia internacional cabe destacar: *1*) la del Tribunal Europeo de Derechos Humanos; en especial los casos "Klass", "Malone", "Kruslin" y "Huvig", sobre intercepciones telefónicas; el caso "Leander" sobre el almacenamiento de información personal por las autoridades públicas nacionales, en concreto los almacenados en los ficheros del departamento de seguridad de la policía nacional sueca; y el caso "Gaskin", sobre el derecho de acceso a datos personales, en concreto, a documentos e información sobre la infancia de un huérfano, recogida en el fichero de un orfanato, y *2*) la del Tribunal de justicia de las Comunidades Europeas, que en varias ocasiones se ha pronunciado en favor del respeto y de la protección de los derechos fundamentales recogidos en el Convenio Europeo de Derechos Humanos, por ejemplo, en el caso "Adams", relativo al art. 214 del Tratado de Roma, que impone la obligación a los miembros de las instituciones comunitarias, a los funcionarios y agentes, de no divulgar las informaciones o datos sobre empresas obtenidos en ejercicio de sus cargos y están amparados por el secreto profesional (Olga Estadella Yuste, *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos, Madrid, 1995, p. 39 a 75).

[2] G. Garzón Clariana, "La informatización de la sociedad y derecho de gentes". Cursos de Derecho Internacional de Vitoria–Gasteiz, Servicio De. Univ. País Vasco, 1983, p. 119, citado por Olga Estadella Yuste, *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos, Madrid, 1995, p. 30.

Asamblea General de la ONU n° 45/95, de 1990), se prevé expresamente el deber de establecer, en los ámbitos nacionales y por vía legislativa, una autoridad imparcial e independiente que se encargue de controlar el respeto de los principios enunciados en el documento, y para el caso de violación de las disposiciones de la legislación interna promulgada en virtud de tales principios, el deber de establecer sanciones penales y de otro tipo así como recursos individuales apropiados (principio rector nº 8, "Control y sanciones" [3]).

Ya en el plano regional europeo el Convenio Europeo de 1981 establece, en su art. 8º ("Medidas adicionales de seguridad para la persona registrada"), inc. *d*, que cualquier persona deberá contar con un remedio si en el pedido de confirmación o, en su caso, comunicación, rectificación o borrado, no se hubiera obrado de acuerdo a lo establecido en el artículo; el art. 10 ("Sanciones y remedios") dice que cada Estado parte se compromete a establecer sanciones apropiadas y remedios ante las violaciones de las provisiones del derecho doméstico, a fin de efectivizar los principios básicos de la protección de datos.

En similar inteligencia, la Directiva 95/46/CE sobre protección de datos personales indica que las legislaciones nacionales deben prever un recurso judicial para los casos en que el responsable del tratamiento de datos no respete los derechos de los interesados (ap. 55 del preámbulo y art. 22).

Con respecto a la autoridad de control, establece que los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación de las normas sobre protección de datos, e indica que una autoridad de control en cada Estado miembro constituye un elemento esencial de la protección que ejerza sus funciones con plena independencia y disponga de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio (numerales 62 y 63 del preámbulo y art. 28).

En los capítulos VI ("Autoridad de control y Grupo de protección de las personas en lo que respecta al tratamiento de datos personales") y VII ("Medidas de ejecución comunitarias"), se dispone lo siguiente:

1) Respecto de la autoridad de control, se indica expresamente en el art. 28 que los Estados miembros dispondrán que una o más autoridades públicas que ejerzan las funciones que le son atribuidas con total independencia, se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la directiva.

Se establece, además, la obligación de consultar a dicha autoridad en el momento de elaborar medidas reglamentarias o administrativas referentes a la protección de los derechos y libertades de las personas en materia de tratamiento de datos de carácter personal, y que ella dispondrá de las siguientes facultades:

a) Poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control.

b) Poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, y garantizar su publicación adecuada, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o la facultad de prohibir provisional o definitivamente un tratamiento, o de dirigir una advertencia o amonestación al responsable del tratamiento o de someter la cuestión a los parlamentos u otras instituciones políticas nacionales.

c) Capacidad procesal en caso de infracciones a las normas nacionales adoptadas en aplicación de la directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

Se aclara que las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional, y que aquella será competente para ejercer en el territorio de su propio Estado miembro estas facultades, pudiendo ser incluso instada por una autoridad de otro Estado miembro.

Entre las obligaciones de la autoridad de control, se establece que se ocupará de:

a) Las peticiones relacionadas con la protección de derechos y libertades en materia de tratamiento de datos personales, debiendo informar del curso dado a éstas.

b) Las solicitudes de verificación de la licitud de un tratamiento cuando sean aplicables las disposiciones nacionales en virtud del art. 13 de la directiva (excepciones y limitaciones al alcance de las obligaciones y los derechos), debiendo informar que tal verificación ha tenido lugar.

---

[3] Principio rector nº 8 ("Control y sanciones"). "Cada legislación debería designar a la autoridad que, de conformidad con el sistema jurídico interno, se encargue de controlar el respeto de los principios anteriormente enunciados. Dicha autoridad debería ofrecer garantías de imparcialidad, de independencia con respecto a las personas u organismos responsables del procesamiento de los datos o de su aplicación, y de competencia técnica. En caso de violación de las disposiciones de la legislación interna promulgada en virtud de los principios anteriormente enunciados, deberían preverse sanciones penales y de otro tipo así como recursos individuales apropiados".

c) Presentar periódicamente un informe sobre sus actividades, que será publicado.

Se refiere, por último, a la relación entre las diversas autoridades de control y les indica que cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil, y que los Estados parte dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso.

Ahora bien: no todas las legislaciones locales –explica Estadella Yuste– prevén que los individuos puedan reclamar el cumplimiento de sus derechos ante una autoridad nacional específica y ante los tribunales ordinarios civiles o administrativos. En aquellos países que siguen una legislación sectorial, y que carecen de autoridad nacional, los individuos tendrán que recurrir a los tribunales ordinarios. En los países con legislación ómnibus, es norma general que la primera demanda por violación de los derechos individuales sobre protección de datos se realice frente a la autoridad nacional, quien estudiará sus términos así como las argumentaciones del titular del fichero.

Normalmente, la mayoría de las legislaciones internas permiten acudir a los tribunales ordinarios civiles o administrativos en apelación a la decisión de la autoridad nacional, o bien por acceso directo en casos determinados. Algunas de las desventajas de prever la vía judicial para garantizar los derechos individuales de forma prioritaria o exclusiva es que la resolución del asunto puede resultar lenta y costosa, sobre todo cuando es necesario aportar dictámenes periciales para arribar a ella, aspecto que puede facilitar la alteración o destrucción de los ficheros[4].

En el particular caso de Indoiberoamérica –así la denominaba el notable jurista Pablo Lucas Verdú para reconocer la preexistencia indígena en estas tierras- ha abordado inicialmente de manera bastante heterogénea la regulación de los diversos contenidos del derecho *de* la protección de datos a partir de un tardío despliegue que, sin perjuicio de algunos antecedentes de la década anterior, comenzó decididamente en la de los años 1990, impulsado por el gradual retorno de sus países a la democracia y por la incorporación en el plano constitucional de la acción de hábeas data, en la Constitución del Brasil de 1988.

Tales diferencias han llevado a que académicamente se postule una solución regional, al estilo europeo pero dentro del ámbito de la OEA, que compatibilice todas las regulaciones nacionales, homogeneizándose así "desde arriba" tales contenidos en la región. Los intentos hasta el momento han sido vanos, pero cabe mencionar que al ya conocido y obsoleto "Anteproyecto de Convención Americana sobre Autodeterminación Informativa" de 1997, comenzaron a sumársele otros documentos más recientes que en definitiva dan anclaje a una futura norma regional: la creación de la Red Iberoamericana de Protección de Datos (La Antigua, junio de 2003) y la Declaración de Santa Cruz de la Sierra (Bolivia, noviembre de 2003), adoptada por los jefes de Estado y de Gobiernos Iberoamericanos, a tenor de cuyo texto (núm. 45) se reconoció el rango de derecho fundamental del derecho a la protección de los datos y se destacó la importancia tanto de las iniciativas regulatorias iberoamericanas, como de la creación de la Red Iberoamericana de Protección de Datos, la cual ha producido invalorables eventos, acciones y documentos que contribuyen a la consolidación y desarrollo del derecho *de* y *a* la protección de datos en la región.

En la evolución normativa regional, el lento e inconcluso proceso se inició con la incorporación de normas constitucionales, que primeramente fueron inspiradas en las disposiciones constitucionales "setentistas" de Portugal (art. 35) y España (art. 18), apuntando primordialmente a la protección de la intimidad frente a la informática (Constitución de la provincia argentina de Córdoba, de 1986) o a garantizar el acceso a los datos en poder del Estado (art. 31 de la Constitución de Guatemala de 1985).

Las posteriores regulaciones constitucionales se refirieron más concretamente a aspectos del derecho de la protección de datos ya con independencia de la protección de la intimidad frente al fenómeno informático, mereciendo destacarse las siguientes regulaciones nacionales en las siguientes constituciones y sus reformas: Brasil (1988, arts. 5, LXXII y LXXVII, 102, II; 105, I,b, 109, VIII y 121, 3), Colombia (1991/2003, art. 15), Paraguay (1992, art. 135), Nicaragua (1993, art. 26), Perú (1993/1994, arts. 2 inc. 5 y 200), Argentina (1994, art. 43), Ecuador (1996/1998, art. 94, 2008, arts. 40, 66, 216 y 436), Venezuela (1999, arts. 28 y 281), Bolivia (2004, art. 23 y 2009, arts. 130 y 131), México (2007/2009, arts 6, 16 y 73). y República Dominicana (2010, art. 44).

Pese a ello, rápidamente las regulaciones fueron adquiriendo rasgos autóctonos, a partir del reconocimiento, ora de facultades propias del derecho a la protección de datos, ora de reglas específicas para procesos judiciales preexistentes o de la creación de procesos judiciales específicos para la protección de los datos de carácter personal, denominados o no hábeas data.

Ya en el plano subconstitucional, han sido dictadas varias leyes, pero pese a que se

[4] Olga Estadella Yuste, *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos, Madrid, 1995, p. 130 y 131.

verifica actualmente una gran inquietud en los países del área por dictar regulaciones al respecto -la mayoría de los países de la región han encarado en sus parlamentos diversos proyectos de normas al estilo europeo-, la realidad dista por mucho de ser satisfactoria, pues hasta el presente muy pocas de esas leyes han sido aprobadas, mereciendo destacarse las de Chile (ley n° 19.628, de 1999); Argentina (ley n° 25.326, de 2000, reglamentada mediante decreto nº 1558/01), Uruguay (ley n° 18.331, de 2008, reglamentada mediante decreto de 31/8/09), México (ley federal de acceso a la información pública, y ley federal de protección de datos en poder de particulares, de 2010), Colombia, (ley n° 184 de 2010), Perú (ley n° 29.733, de 2011) y Costa Rica (ley n° 8968, de 2011).

De otro lado, se han dictado leyes sectoriales, entre muchas otras, las de Perú (ley 17.489, de 2001); Uruguay (la ley 17.838 de 2004, sobre informes comerciales incorporó reglas típicas de la protección de datos en general y creó la acción de hábeas data) y las leyes mexicana y brasileña de defensa del consumidor (ley nº 8.078/90, Código de Defensa del Consumidor, arts. 43 y 44, que regulan aspectos de los bancos de datos en las relaciones de consumo, norma a la que deben sumarse las leyes nº 9.296/96 y nº 10.217/01 que reglamentan la intercepción telefónica y la grabación ambiental y el tratamiento de los datos derivados de esas actividades; la ley nº 105/01, que permite que las autoridades administrativas quiebren el secreto bancario en casos de delitos graves, sin autorización judicial, y la ley nº 9.613/98, de blanqueo de capital, que define delitos específicos).

Hecha esta necesaria introducción, nos ocuparemos del tratamiento concreto del caso argentino.

2. El derecho a la protección de datos en la Argentina

Argentina es un país con un sistema federal con fuertes rasgos de unitarismo. En este sentido, las facultades concedidas en la Constitución nacional al Congreso de la federación para dictar la legislación de fondo (art. 75, inc. 12, 121 y 126) son especialmente amplias si se las compara con el sistema estadounidense.

De otro lado, los estados federados mantienen por regla las potestades de juzgamiento respecto de los actos regidos por tales normas de fondo (arts. 5 y 75, inc. 12) y asimismo ejercen el control sobre sus propias instituciones (arts. 121 a 123).

Este esquema normativo da origen a un fenómeno particular que torna más complejo el control administrativo y judicial del derecho a la protección de datos, ya que si bien el Congreso nacional puede dictar una serie de reglas de fondo aplicables en todo el país, no puede establecer un órgano de control con facultades en todo el territorio nacional (sólo puede controlar los bancos de datos de titularidad pública nacional y los que estén interconectados en redes interjurisdiccionales nacionales o internacionales, conforme lo expresa el art. 44 de la ley 25.326[5]) y tampoco puede regular los procesos judiciales propios de los estados federados, pudiendo sólo establecer la jurisdicción de los juzgados federales con asiento en los estados federados sobre bancos de datos de titularidad pública nacional y los privados interconectados (art. 36, ley 25.326[6]).

De tal suerte, los bancos de datos de titularidad pública provincial o municipal y los bancos de titularidad privada no interconectados en redes interjurisdiccionales sólo pueden ser controlados a través de los órganos administrativos y judiciales creados en los estados federados.

2.1. Marco normativo.

A partir de la incorporación, en la Constitución federal, de la acción de hábeas data (art. 43, tercer párrafo[7]), y de un importantísimo despliegue doctrinario y jurisprudencial, en 2000 se dictó la ley de protección de datos personales (n° 25.326), basada en la ya por entonces derogada Lortad española de 1992.

Esta ley fue inmediatamente reglamentada por el decreto n° 1558/01, reformada tangencialmente en 2008 por ley 26.343 que impuso un blanqueo de morosos, y también

---

[5] "Art. 44**.** – (Ámbito de aplicación). Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional.

"Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.

"La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional."

[6] "Art. 36. — (Competencia). Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

"Procederá la competencia federal:

"a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y

"b) cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales."

[7] "Art. 43.–[...] Toda persona podrá interponer esta acción (se refiere a la de amparo) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

cuenta con reglamentación de segundo grado a partir de las disposiciones emanadas de su órgano de control.

La ley de protección de datos es plenamente aplicable, en cuanto a sus principios generales, en todo el país, pero tiene algunas limitaciones importantes, dado que: a) el órgano de control instituido por la ley sólo tiene jurisdicción sobre bancos de datos del sector público federal y sobre bancos de datos de titularidad privada interconectados en redes interjurisdiccionales (esto es, los que exceden del tratamiento dentro de un estado federado); y además técnicamente es dependiente del Poder Ejecutivo y b) el proceso de hábeas data, como vía de encauzamiento de la acción de protección de los datos personales, sólo pudo ser regulado para los juicios que se tramiten ante el fuero federal, pues la materia procesal está reservado a los estados federados, que por regla general no lo han regulado ante la falta de urgencia ya que se utilizan para encauzar a la acción las reglas preexistentes del amparo.

Es decir, si bien la ley es aplicable en lo relativo a los principios generales del tratamiento de datos en todo el país, para que la tutela sea completa se requiere: a) el dictado de leyes en los estados federados que dispongan la creación de órganos de control que tengan jurisdicción sobre los bancos de datos que están fuera de la competencia del órgano de control federal, y b) la adecuación de las normativas procesales locales preexistentes a fin de alojar, con sus particulares características y requerimientos, a este nuevo proceso constitucional. A ello cabe agregar que restaría –y ello no es menos importante- modificar el diseño del órgano de control para otorgarle independencia suficiente respecto del Poder Ejecutivo y obviamente también de cualquiera de los demás poderes del Estado.

2.2. La Protección judicial y administrativa en el plano federal y en los estados federados.

Transcurrida la primera década desde la aprobación de la ley federal de protección de datos, de los 24 estados federados, cinco dictaron leyes que abordan desde algún ángulo la tutela del derecho a la protección de datos[8], y sólo uno –la Ciudad Autónoma de Buenos Aires- estableció su órgano de control (la Defensoría del Pueblo de la Ciudad de Buenos Aires), además de regular la acción de hábeas data -Misiones y Neuquén establecieron órganos de control pero no han entrado en funcionamiento-.

Las restantes provincias se limitaron a este último aspecto, con la adición, en algunos casos, del procedimiento prejudicial de acceso y control sobre los datos (v.gr., Chubut), y algunas reglas sobre el tratamiento de datos para los bancos de datos locales (p. ej., San Juan, que obliga a éstos a inscribirse en el Registro Público de Comercio y en la Dirección de Defensa del Consumidor).

Del cuadro predescripto se observa una persistencia generalizada en las falencias regulatorias, que en alguna medida ha sido provocada también por la eficacia de los mecanismos judiciales de tutela, ya que el Poder Judicial, en aplicación de los principios emanados del art. 43 constitucional federal (operativo en toda la República), ha dado respuesta acabada no sólo a la tutela efectiva del derecho a la protección de datos allí contenido por la vía del hábeas data, sino también a la debida reparación a los lesionados por el tratamiento indebido de sus datos personales.

Las falencias más notorias del sistema argentino de protección de datos fueron observadas puntualmente en el dictamen del Grupo de Trabajo del art. 29 de la Directiva 95/46/CE, de 2002[9], en el cual se evaluó la situación de la Argentina frente al tratamiento de datos (lo que implicó valorar tanto la compatibilidad de sus normas, su doctrina y su jurisprudencia, como el plano fáctico), y se aconsejó otorgarle el status de país extracomunitario con nivel de protección adecuado a los fines de la transmisión internacional de datos, pero el reconocimiento con tal carácter (el primero en Latinoamérica en obtener tal certificación, en 2003) no le fue concedido sin reservas.

En efecto, en el referido dictamen se objetó, por un lado, la ausencia -por entonces total y por cierto hoy todavía predominante– de órganos de control de los estados federados, y, por el otro, la falta de independencia del órgano de control nacional –este aspecto sólo se consideró respecto de la normativa vigente, pues poco podía evaluarse sobre su desempeño dado que apenas estaba comenzando a funcionar–, toda vez que la ley 25.326 encomendó tal rol a una mera dirección -la Dirección Nacional de Protección de Datos- ubicada en la estructura administrativa del Poder Ejecutivo y como apéndice de la Secretaría de Justicia y Asuntos Legislativos (luego Subsecretaría de Asuntos Registrales de la Secretaría de Justicia), a su vez dependiente del Ministerio de Justicia y Derechos Humanos.

Estas observaciones, que a simple vista pudieran parecer meramente formales, en realidad no son tales, pues hay fundamentos relevantes y de peso para sostener la necesidad de producir urgentemente las adecuaciones sugeridas por el citado dictamen

---

[8] En concreto, se dictaron las leyes n° 4244, de Chubut (1996); n° 4360, del Chaco (1996); n° 3246, de Río Negro (1998); n° 7447, de San Juan (2004), y n° 1845, de la Ciudad Autónoma de Buenos Aires (2005).

[9] http://europa.eu.int/comm/internalmarket/en/dataprot/wpdocs/index.htm.

del Grupo de Trabajo del art. 29 de la Directiva Europea 95/46.

2.2.1. EL CONTROL ADMINISTRATIVO EN GENERAL Y EN LOS PLANOS FEDERAL Y LOCAL.

La cuestión del diseño, funciones y ubicación del órgano de control, en aras de su necesaria independencia no es menor, pues la labor de aquél es relevante dado que no sólo opera como complemento de la actividad de los tribunales, sino también en sustitución o prevención de ésta, como se evidencia con toda claridad en el contraste existente actualmente entre los países que tempranamente dictaron normas sobre protección de datos de carácter personal y establecieron órganos de control y aquellos que, sin regulación específica alguna, dejaron la mayor actividad de control a cargo de los tribunales.

Al respecto, Pérez Luño destaca las bondades de los sistemas que incorporaron órganos de control específico, el sistema del *ombudsman* en defensa de los derechos y libertades de la tercera generación ha adquirido tal protagonismo que actualmente se diversifica en una serie de variantes que llegan a ser formulados unipersonales o colegiados, y hasta ser específicamente dirigidos a la protección de los ciudadanos respecto al tratamiento informatizado de datos personales; es decir, a hacer efectivo el hábeas data.

Entre las ventajas que ofrece el sistema del *ombudsman* para la protección efectiva de los derechos humanos pueden citarse las referidas a las funciones siguientes: 1) Función dinamizadora, adaptadora y de reciclaje de los derechos fundamentales, realizada básicamente a través de los informes periódicos presentados ante los Parlamentos de los que son comisionados. 2) Función orientadora de los ciudadanos, agilizando y clarificando los procedimientos de tutela de las libertades. 3) Función preventiva de las lesiones a los derechos humanos, evitando agresiones y daños de difícil o imposible reparación en el ejercicio de tales derechos; ya que al ejercicio de las libertades es de cabal aplicación el célebre adagio latino: *melius est prevenire quam reprimere*[10].

Analizando la formulación en este aspecto de las primeras normas europeas, indica Fappiano que la primera ley de protección de datos, del Land de Hesse (República Federal de Alemania) creó la figura del comisario para la protección de datos, especie de *ombudsman*, llamado luego comisario federal al dictarse la *Datenschutz* Federal (27/1/77), quien debe velar por el cumplimiento de la norma y recibir quejas de los afectados. De acuerdo con el art. 17, es designado por el presidente de la República Federal a propuesta del gobierno federal, es independiente en el desempeño de su cargo y se encuentra sometido sólo a la ley, sin perjuicio del derecho de supervisión por parte del gobierno federal.

En el caso estadounidense, la *Privacy Act* de 1974 no establece una institución unipersonal o colegiada encargada de la supervisión y control de la aplicación de la norma, por lo que ante la afección de alguno de los derechos se debe acudir directamente al Poder Judicial.

La ley francesa de protección de datos (6/1/78) establece un órgano encargado de vigilar su aplicación y recibir las denuncias de los titulares de los datos en caso de que se les impidiera el acceso o se negaran a la intervención del dato. Pero, a diferencia de la ley alemana, es un órgano colegiado: la Comisión Nacional de la Informática y de las Libertades (compuesto por dos diputados, dos senadores, miembros del Tribunal de Casación y del Tribunal de Cuentas, dos personalidades solventes en la materia electos por el presidente de las cámaras, etc.), se encarga de velar por el respeto de los preceptos de la ley, especialmente informando a todos los interesados de sus derechos y obligaciones, concertándose con ellos y controlando las aplicaciones de la informática a los tratamientos de informaciones de carácter personal (art. 6º). Es un organismo autónomo, compuesto de diecisiete miembros, siendo incompatible la condición de miembro de la Comisión con la de miembro del Gobierno o con el ejercicio de funciones o la posesión de participación alguna en las empresas que concurran a la fabricación de material utilizado en informática o en telecomunicaciones o al suministro de servicios en esas áreas[11].

También Portugal cuenta con un organismo público autónomo integrado por siete miembros (tres por el Parlamento, dos magistrados y dos personalidades de reconocido prestigio elegidas por el gobierno); Austria tiene dos órganos de control: la Comisión y el Consejo de Protección de Datos (con representantes de los partidos políticos, de los Estados regionales y del Poder Judicial).

En el caso de España, la Lortad (Ley Orgánica sobre el Régimen de Tratamiento Automatizado de Datos) de 1992 (reformada por la LOPDP en 1999) creó la Agencia de Protección de Datos (hoy Agencia Española de Protección de Datos), como ente de

---

[10] Antonio Pérez Luño, *Del hábeas corpus al hábeas data*, citado por Villalobos, *Derecho de la informática*, en *"Temas para Universidades, Facultades de Derecho y Ciencias Políticas"*, p. 135 y 136.

[11] Oscar Luján Fappiano, *Hábeas data: una aproximación a su problemática*, en "Liber Amicorum: Héctor Fix Zamudio", vol. I, p. 643 y siguientes.

derecho público con personalidad propia, plena capacidad pública y privada e independencia de las administraciones públicas en ejercicio de sus funciones, que se rige por un estatuto propio –que debe corresponderse con la ley orgánica 30/92, de creación del órgano– y tiene competencia en todo el territorio nacional. Está a cargo de un director, nombrado por real decreto, por un período de cuatro años, elegido entre quienes componen el Consejo Consultivo del ente, y no recibe instrucciones para su desempeño. Además de esta autoridad, la misma ley prevé la instalación de agencias en las comunidades autónomas, que coordinan sus funciones con la autoridad nacional, y cuyas competencias no son meramente residuales.

Entre otros antecedentes, Canadá cuenta con un *privacy commissioner* y Noruega con su *datalisynet*. En Alemania actúan a escala federal y en los *lander* que cuentan con leyes propias de protección de datos, los comisarios para la protección de datos (*Datenschutzbeauftragten*) y en Francia, como se dijo, a partir de su ley sobre informática, archivos y libertades de 1978, se creó una *Commission Nationale de l'Informatique et des Libertés* compuesta por diecisiete miembros y con algunas competencias similares a la figura del *médiateur* (institución francesa equivalente al *ombudsman*) respecto de la vigilancia a los departamentos administrativos informatizados. También Gran Bretaña cuenta con instituciones como el *Registrer* y el *Data Protector*, un tribunal especializado en la tutela de los derechos cívicos frente a eventuales abusos informáticos.

La experiencia europea demostró la utilidad del sistema protector cuando cuenta con autoridad de control (unipersonal o colegiada), y por ello las reglas globales y regionales relativas a la protección de datos establecen la necesidad de incorporarlo en la legislación nacional. Bien lo ha destacado al respecto el Tribunal Constitucional español, en la sentencia 290-2000[12]

---

[12] Sentencia del TC nº 290/2000, de 30 de noviembre de 2000, sobre recursos de inconstitucionalidad contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal, en la que sostuvo:

: "8. En lo que respecta en segundo término a la Agencia de Protección de Datos que ha creado el Título VI de la Lortad, ha de comenzarse señalando que en las regulaciones legales adoptadas antes de la entrada en vigor de nuestra Constitución por varios Estados europeos con la finalidad de proteger los datos personales frente a los peligros de la informática (Ley sueca de 11 de mayo de 1973, Ley de la República Federal de Alemania, de 22 de enero de 1977, Ley francesa de 6 de enero de 1978, Ley noruega de 8 de junio de 1978), también está presente un elemento institucional. Pues dichas regulaciones, pese a las diversas denominaciones y dependencias orgánicas que establecen, tienen en común el haber creado instituciones especializadas de Derecho público, a las que se atribuyen diversas funciones de control sobre los ficheros de datos personales susceptibles de tratamiento automatizado, tanto de titularidad pública como privada.

"Pues bien, la Lortad ha establecido un "régimen de protección de datos de carácter personal" respecto de los que figuren en ficheros automatizados, tanto de titularidad pública como privada, así como las modalidades de su uso posterior (art. 2). Y en dicho régimen su dimensión institucional es la referida a la Agencia de Protección de Datos y a los órganos que en ella se integran, tanto de dirección (Director y Consejo Consultivo, arts. 35 y 37 Lortad) como operativos (Registro General de Protección de Datos e Inspección de Protección de Datos, arts. 38 de la Ley y 11 del Estatuto de la Agencia de Protección de Datos). Habiendo configurado el legislador a esta Agencia con unos rasgos específicos, pues se trata de "un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones" (art. 34.2 Lortad).

"En lo que respecta a las funciones y potestades atribuidas a la Agencia de Protección de Datos, el apartado a) del art. 36 Lortad ofrece una caracterización general de las primeras al encomendar a la Agencia la función general de "Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial respecto a los derechos de información, acceso, rectificación y cancelación de datos". Y en cuanto especificación de esta función de carácter tuitivo en orden a la protección de datos personales, los restantes apartados del citado precepto le atribuyen tanto funciones de intervención o control respecto a ciertos sujetos y actividades como funciones registrales y consultivas. Siendo de destacar, en cuanto a las primeras, la de emitir las preceptivas autorizaciones previstas en la Ley o en las disposiciones de desarrollo de ésta (apartado b); la de ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de ficheros cuando no se ajusten a lo previsto en la Lortad (apartado f); la de velar por la publicidad de la existencia de los ficheros, a cuyo efecto publicará periódicamente una relación periódica de los mismos (apartado j); la de ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos y las de cooperación internacional en esta materia (art. 36, apartado 1) y las relativas a la recogida y secreto de datos estadísticos, dictando instrucciones sobre las condiciones de seguridad de los ficheros [art. 36, apartado m)].

"Se trata, pues, de un conjunto de funciones especializadas en cuanto a su objeto, la protección de los datos personales y, además, de funciones de carácter público, como se expresa en el art. 34.1 Lortad al determinar que la Agencia de Protección de Datos actuará de conformidad con la Ley de Procedimiento Administrativo, sin perjuicio de que sus adquisiciones patrimoniales y contratación estén sometidas al Derecho privado.

"En correspondencia con el carácter público de sus funciones, la Agencia de Protección de Datos dispone de potestades administrativas expresamente atribuidas por dicha Ley.

"En primer lugar, la potestad de investigación o de inspección que le reconoce el art. 39 para obtener información y, en su caso, pruebas sobre los hechos que contravengan lo dispuesto en la Lortad. En segundo término, la potestad sancionadora, que la Agencia de Protección de Datos ha de ejercer en los términos previstos en el Título VII [art. 36, apartado g)], con la particularidad, cuando se trate de infracciones de una Administración Pública, que tal potestad queda limitada a la facultad de dictar una resolución indicando las medidas que han de adoptarse para corregir el incumplimiento de las previsiones legales en esta materia (art. 45). En tercer lugar, una potestad de resolución de las reclamaciones de los afectados por incumplimiento de las previsiones de dicha Ley [art. 36, apartado d)] en relación con el art. 17.1, con sujeción al procedimiento establecido por el Real Decreto 1332/1994, de 20 de julio. Y, por último, una potestad normativa, ceñida en lo esencial a dictar las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Lortad [art. 36, apartado c) y m) *in fine*], con miras a su debida aplicación en ámbitos determinados de actividad.

"9. Por último, de lo que se acaba de exponer se desprende un rasgo significativo de la Agencia de Protección de Datos: el carácter básicamente preventivo de sus funciones en orden a la protección de datos personales. Un rasgo caracterizador que es común a las instituciones especializadas existentes en los países de nuestro entorno y al que ha hecho referencia la Exposición de Motivos de la Lortad al afirmar que esta disposición está guiada "por la idea de implantar mecanismos cautelares que prevengan las violaciones" de los derechos fundamentales.

"En efecto, al dar cumplimiento al mandato contenido en el art. 18.4 CE, el legislador, sin excluir en modo alguno el recurso último a los órganos jurisdiccionales para la tutela de los derechos individuales, como se determina en los apartados 2 a 5 del art. 17 Lortad, no ha querido sin embargo que la protección de datos personales frente al uso de la informática se lleve a cabo exclusivamente en la vía judicial, esto es, cuando ya se ha producido una lesión del derecho fundamental.

"Por el contrario, ha querido que dicha protección se lleve a cabo mediante el ejercicio por la Agencia de Protección de Datos, con carácter básicamente preventivo, de las funciones de control de los ficheros tanto de titularidad pública como privada que la Lortad le atribuye y, en su caso, a través de las reclamaciones de los afectados ante la Agencia de Protección de Datos (art. 17.1), las que provocarán la posterior actuación de este órgano.

"Por lo que cabe estimar que existe una correspondencia entre las funciones y potestades que la Lortad ha atribuido a la Agencia de Protección de Datos y el carácter preventivo de sus actuaciones. Pues es este carácter tuitivo o preventivo el que, en última instancia,

En América Latina, el control se ha ido perfilando homogéneamente hacia un modelo de escasa independencia –al menos desde lo formal- por cuanto a partir del "modelo argentino", al que nos referiremos luego, se ha instalado la idea de establecer un órgano de control instalado en la órbita del Poder Ejecutivo y en definitiva sometido en buena medida éste, tal como surge de las leyes uruguaya, peruana, colombiana y costarricense, y en algunos casos con funciones aún muy menores a las mínimamente necesarias, como ocurre en el caso de la ley chilena.

En el caso argentino, en el plano federal, la ley 25.326 establece en su Capítulo V ("Control"), a través de dos artículos, las pautas esenciales del control administrativo en la aplicación de la ley.

El art. 29 se ocupa del diseño, las obligaciones, funciones y atribuciones del órgano de control, las que consisten no sólo en el despliegue de facultades que entrañan verdaderos deberes de control de los bancos de datos sujetos a la jurisdicción del órgano –a los que puede imponer sanciones administrativas de diversa índole–, sino también en la prestación de servicios a la comunidad, que llegan incluso hasta a su defensa judicial, ya que se faculta al titular del órgano a constituirse en querellante en las acciones penales que los afectados inicien por violación a los derechos reconocidos por la ley.

Por su parte, el art. 30 promueve la elaboración de códigos de conducta por parte de las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada[13]. Estas reglas, que no son sino normas autorregulatorias de buena práctica profesional que funcionan como forma de autocontrol sectorial, pueden ser homologadas y controladas, en cuanto a su cumplimiento, por la autoridad administrativa de aplicación de la ley.

Este rol de control sobre el cumplimiento de los principios y derechos reconocidos por la ley se completa en los dos capítulos siguientes ("Sanciones" y "Acción de protección de los datos personales"), donde la ley regula, por un lado, las sanciones administrativas (para cuya aplicación se faculta al órgano de control) y las penales (a cargo de los jueces respectivos); y por el otro, una acción especial de protección de datos personales (a la que también denomina "hábeas data"), ejercible principalmente por el titular de los datos frente a determinados registros, cuando los derechos reconocidos en la ley se vieren conculcados.

Como se expresara supra, el control administrativo establecido a nivel nacional no alcanza a todos los sistemas de información a los que están destinadas las reglas emanadas del art. 43 constitucional y de la ley 25.326 que se aplican en todo el país, ya que el órgano de control nacional no tiene facultades para controlar los bancos de datos de titularidad pública de los estados federados ni los de titularidad privada que no se encuentren interconectados en redes interjurisdiccionales, que deben ser tutelados administrativamente por los órganos de control locales, donde la regulación específica sólo se produjo en tres estados, y sólo en uno está en funcionamiento: la ciudad de Buenos Aires, que, como se dijo, puso en manos de su Defensoría del Pueblo la tutela de los datos personales de sus habitantes.

En cuanto al órgano federal, el art. 29 de la ley 25.326 establece su diseño y funciones y difiere su conformación definitiva y funcionamiento a la reglamentación[14]. El

---

justifica la atribución de tales funciones y potestades a la Agencia de Protección de Datos para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos personales en relación con todos los ficheros, ya sea de titularidad pública o privada."

[13] "Art. 30. — (Códigos de conducta). 1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, 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 establecidos en la presente ley.

"2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia."

Esta norma fue reglamentada por el decreto 1558/01, que al respecto establece: "Art. 30.- La DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES alentará la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por la Ley Nº 25.326 y esta reglamentación.

"Las asociaciones de profesionales y las demás organizaciones representantes de otras categorías de responsables o usuarios de archivos, registros, bases o bancos de datos públicos o privados, que hayan elaborado proyectos de códigos éticos, o que tengan la intención de modificar o prorrogar códigos nacionales existentes, podrán someterlos a consideración de la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, la cual aprobará el ordenamiento o sugerirá las correcciones que se estimen necesarias para su aprobación."

[14] Art. 29. — (Órgano de Control).

1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

texto del artículo originalmente aprobado por el Congreso resultó vetado por el Poder Ejecutivo en sus apartados 2 y 3[15], lo que implicó un severo cercenamiento de su ya limitada independencia

Cuando fuera sometida a discusión la cuestión del diseño y ubicación del órgano de control en el debate parlamentario de la que luego sería la ley 25.326, después de ser evaluadas las diversas posibilidades regulatorias[16] se optó por un órgano de control específico de tipo unipersonal, pero con independencia recortada, pues aunque expresamente se lo dotaba de autonomía funcional y se lo perfilaba como órgano descentralizado, ello se pensó dentro del ámbito del Ministerio de Justicia y Derechos Humanos, y la designación de su titular se encargó al Poder Ejecutivo, con acuerdo del Senado.

Con el veto presidencial parcial del art. 29, realizado mediante decreto n° 995/00 –fundado en cuestiones presupuestarias y en las facultades que la propia ley le confería para diseñar el órgano respectivo[17]-, el órgano pergeñado quedó desvirtuado en su fortaleza por varios motivos que exceden al de su dependencia funcional y se vinculan

---

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;

e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.

[15] Los apartados respectivos disponían lo siguiente: "2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.

"3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

"El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones."

Cabe aquí advertir que pese a que en muchas publicaciones aparece como no vetado el segundo párrafo del ap. 3 del art. 29 de la ley 25.326, en realidad lo está, ya que el veto fue mal publicado en el Boletín Oficial.

[16] Ver al respecto las intervenciones del Senador Branda, quien bregó por un órgano independiente y colegiado (Antecedentes Parlamentarios", 2001–A–275 y 276); del Senador Berhongaray, quien se inclinó por adjudicarle el control al defensor del pueblo ("Antecedentes Parlamentarios", 2001–A–270); del Senador Villarroel, quien insistió en no delegar al Ejecutivo la conformación del órgano de control ("Antecedentes Parlamentarios", 2001–A–264), y del Senador López, quien indicó su pretensión acerca de que el órgano de control sea autónomo e independiente, y no adscripto a la órbita de funcionamiento del Poder Ejecutivo, con representantes de las Cámaras de Diputados y de Senadores, de la Corte Suprema y de la Fiscalía Nacional de Investigaciones Administrativas ("Antecedentes Parlamentarios", 2001–A–381).

El Senador Menem, uno de los autores del proyecto original, descartó los fundamentos esgrimidos y justificó la orientación escogida, sosteniendo que aun ante las distintas propuestas que colocan al órgano de control al margen del Poder Ejecutivo, debe estar en la esfera de su competencia, ya que a éste le corresponde la administración general del país, y aquí se trata de desarrollar una eminente función administrativa de regulación y control, en especial respecto de los bancos de datos públicos. Considerando las inquietudes planteadas en el dictamen en disidencia se acepta reforzar la independencia técnica y funcional, teniendo en cuenta que al órgano de control también le corresponderá ejercer sus atribuciones respecto del Poder Ejecutivo, y se propone que el director sea designado por el Ejecutivo con acuerdo del Senado, estableciendo legalmente el período de duración en el cargo y su inamovilidad. Por lo demás, se dejan al Poder Ejecutivo los detalles respecto de la regulación burocrática que corresponda, teniendo en cuenta la reforma administrativa en marcha. Esto no excluye la participación del defensor del pueblo que, como es sabido, es un órgano del Congreso de la Nación que actúa con independencia funcional y autarquía financiera. Se resigna abundar en detalles a fin de que sea la reglamentación la que complete el tema. Insistió en una segunda intervención al contestarle al Senador López que advertía cierta desconfianza sobre las facultades de control del Poder Ejecutivo, y que la norma proyectada otorgaba una serie de garantías que, de ningún modo, pueden hacer pensar que ese órgano estará sometido a la influencia del Poder Ejecutivo. Remarcó además que al establecerse que el órgano de control tendrá autonomía funcional y que actuará como órgano descentralizado, se establece que será dirigido y administrado por un director designado por el término de cuatro años por el Poder Ejecutivo, con acuerdo del Senado de la Nación. Es decir, se le está dando el tratamiento que hasta hace poco tiempo se tenía para la designación de jueces y que ahora se tiene para la designación de embajadores y de miembros del Banco Central. ("Antecedentes Parlamentarios", 2001–A–363 y 382).

Al ser tratada la norma en Diputados, el dictamen de las comisiones considerado por el cuerpo –que fue aceptado por la Cámara cuando aprobó las modificaciones al artículo– proponía algunas modificaciones al art. 29, pero al volver al Senado se votó en bloque todo el capítulo sin incorporar ninguna de las modificaciones propuestas por la cámara revisora.

[17] Los argumentos del veto fueron los siguientes: a) La constitución del órgano de control como organismo descentralizado habrá de implicar, como toda incorporación de una estructura organizativa de este tipo, un incremento en las erogaciones del Estado nacional para atender su funcionamiento. b) El proyecto de ley no prevé el financiamiento del órgano de control, y la ley 25.237 de presupuesto de la Administración nacional para el ejercicio 2000 y el proyecto de ley de presupuesto nacional para el ejercicio 2001 no contienen previsiones crediticias para su atención. c) La legislación vigente en materia de administración financiera pública determina que todo incremento de gastos debe prever el financiamiento respectivo. d) Se considera pertinente la constitución de un órgano de control que reúna las características organizativas que determine el Poder Ejecutivo nacional de conformidad con la autorización conferida por el art. 45 del proyecto, que establece que debe reglamentar la ley y establecer el organismo dentro de los ciento ochenta días de su promulgación.

con otros aspectos, también esenciales, que tienen que ver precisamente con la forma de elección, requisitos para el cargo, duración y estabilidad de su titular[18].

Así las cosas, se vaciaron prácticamente de contenido las pocas garantías que la norma había establecido en pos de lograr una mínima independencia y la necesaria estabilidad de su director, y aunque ello se pretendió salvar con la reglamentación de la ley, vía el decreto n° 1558/01, tal cosa no ocurrió, pues pese a lo que dispuso la norma[19], el órgano mantiene su dependencia funcional y su director fue sólo una vez designado por concurso público, para el período comprendido entre 2002 y 2006[20].

Como se puede observar, el marco normativo es claramente insuficiente para otorgar garantías mínimas de independencia y eficacia, no sólo porque éstas están consagradas a través de meros decretos –los que, como tales, pueden dejarse sin efecto de la noche a la mañana y sin intervención del Congreso-, sino porque aún cuando cobraran vigencia las partes vetadas de la ley, ello no podría revertir la crítica referida a la dependencia del órgano de control respecto del Poder Ejecutivo por cuanto un órgano inserto en esa estructura no responde a los requerimientos internacionales, lo que amerita, en definitiva rediseñar la autoridad de aplicación conforme a éstos.

En mérito de lo expresado, surge claro que el sistema de control pergeñado originalmente, aún cuando no hubiera sido vetado por el Poder Ejecutivo, en la práctica también hubiera demostrado (aunque en menor medida) una autonomía muy recortada del órgano de control, tal como fue advertido claramente por la Comunidad Europea, que entiende a éste como la clave central del eficaz funcionamiento del sistema de protección.

Cabe resaltar entonces, en este aspecto, la urgente necesidad de que se dicte una reforma sustancial al actual art. 29 de la ley, con un mayor nivel de detalle y quite toda dependencia jerárquica, técnica y económica del órgano de control respecto del Poder Ejecutivo, pues ello conspira decisivamente contra su plena independencia, en especial por tener la labor de controlar una enorme cantidad de registros dependientes de aquél.

El ajuste necesario para revertir la observación internacional, entonces, primeramente depende de la actividad legislativa, toda vez que se requiere una reforma al art. 29 de la ley 25.326 por la que:

a) se diseñe un nuevo órgano de control, preferentemente al estilo europeo (un órgano de control ubicado fuera del Poder Ejecutivo y preferentemente con funciones específicas y excluyentes, como la Agencia Española de Protección de Datos o –en una hipótesis de mínima un defensor del pueblo especializado, por ser ajena a esta institución la concesión de poderes sancionatorios), pues evidentemente no basta para la Comunidad Europea con que el órgano de control demuestre una importante actividad y

---

[18] Los apartados respectivos disponían lo siguiente: "2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.

"3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

"El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones."

Cabe aquí advertir que pese a que en muchas publicaciones aparece como no vetado el segundo párrafo del ap. 3 del art. 29 de la ley 25.326, en realidad lo está, ya que el veto fue mal publicado en el Boletín Oficial.

[19] El art. 29, ap. 1 del decreto citado dispuso: "Créase la Dirección Nacional de Protección de Datos Personales, en el ámbito de la Secretaria De Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos, como órgano de control de la Ley Nº 25.326

"El Director tendrá dedicación exclusiva en su función, ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones."

Y el apartado 2 estableció: "La Dirección Nacional de Protección de Datos Personales se integrará con un Director Nacional, Nivel "A" con Función Ejecutiva I, designado por el Poder Ejecutivo Nacional, por el plazo de cuatro (4) años, debiendo ser seleccionado entre personas con antecedentes en la materia, a cuyo fin facúltase al Ministro de Justicia y Derechos Humanos, o a quien lo sustituya en sus funciones, a efectuar la designación correspondiente, como excepción a lo dispuesto por el Anexo I del Decreto Nº 993/91 y sus modificatorios."

[20] El primer concurso fue convocado por resolución 325/02 del Ministerio de Justicia y Derechos Humanos, y desembocó en la designación del primer director, Dr. Juan Antonio Travieso, mediante decreto 1898/02, y por el plazo de cuatro años.

Con anterioridad a ello, por medio de la res. 17/02 del Ministerio de Justicia y Derechos Humanos (modificada por res. 98/02), ya lo había designado, considerando que cumplía funciones de jefe de Gabinete de Asesores del ministro de Justicia y Derechos Humanos, su dedicación exclusiva a esa jurisdicción y su experiencia en la materia como docente universitario y otros antecedentes de cargos públicos afines. Tal designación fue formalmente objetada por recomendación de la Oficina Anticorrupción del 8/4/02, en la que se aconsejaba convocar a concurso público a fin de ampliar la base de los postulantes, y fruto de tal observación, mediante la res. 325/02, el Ministerio de Justicia y Derechos Humanos convocó al concurso para la selección a fin de cubrir el cargo. Luego de una etapa de preselección el Comité de Evaluación elaboró una terna, de la cual el único votado unánimemente para el cargo fue el doctor Juan A. Travieso, cuya designación tuvo lugar por el decr. 1898/02.

Vencido el período de cuatro años (2002/2006) fue designado por el Poder Ejecutivo nacional mediante decreto n° 779/07, de 21/06/07 (B.O. del 25/06/07), un segundo director (Dr. Francisco José Orue), sin concurso, y de allí el anunciado carácter transitorio de la designación, pues en el decreto se anunció, que, dado que por razones de índole operativa no se ha podido tramitar el proceso de selección para el cargo, y que el mismo deberá ser cubierto "de conformidad con lo previsto en el artículo 29, inciso 2, del Decreto Nº 1558/01". Pese al anuncio, ello nunca aconteció, y el primer director fue nuevamente designado por decreto y sin concurso.

hasta independencia de criterio[21] si existe dependencia jurídica, y

b) se establezcan bases objetivas para la designación del titular del ente de control y se garantice su estabilidad, que hoy sólo está establecida por vía de decreto, pues si bien el art. 29 ap. 3 estipulaba en su primer párrafo que el órgano de control sería dirigido y administrado por un director que duraría cuatro años en sus funciones, y sería designado, entre personas con antecedentes en la materia, por el Poder Ejecutivo con acuerdo del Senado de la Nación, ese párrafo resultó vetado, y lo mismo ocurrió con el segundo párrafo –que tampoco superó el veto presidencial pero no fue publicado como vetado en el Boletín Oficial– en el que se indicaba que el director tendría dedicación exclusiva y estaría alcanzado por las incompatibilidades fijadas para los funcionarios públicos, pudiendo ser removido por el Poder Ejecutivo por mal desempeño de sus funciones.

Por último, cabe recordar que también hay en materia de órganos de control, obligaciones incumplidas por parte de los estados federados, pues a partir de lo dispuesto en el art. 44 de la ley 25.326, queda claro que la autoridad nacional no tiene imperio sobre la totalidad de los bancos de datos existentes en la República, por lo que deben replicarse en los estados federados autoridades de control que completen el espectro protectivo (la única vigente es al de la Ciudad Autónoma de Buenos Aires, que además no reúne las condiciones fijadas por la Comunidad Europea). Ello sigue constituyendo una demora inaceptable, máxime cuando ello está permanentemente motorizado por parte del órgano de control nacional, que tempranamente se volcó a la creación de una red nacional de protección de datos.

2.2.2. EL CONTROL JUDICIAL (FEDERAL Y LOCAL) A TRAVÉS DEL HÁBEAS DATA.

El hábeas data, como acción y como proceso constitucional de corte judicial fue incorporado por el art. 43 constitucional en la última reforma integral a la Carta Federal, realizada en 1994, donde se lo concibió como un amparo especializado. La Corte nacional, en "Urteaga"[22] lo declaró plenamente operativo en toda la República, por lo que los jueces deben aplicarlo aún cuando carezca de reglamentación específica, adaptando los trámites preexistentes a las necesidades del nuevo instituto.

En el ámbito federal, el hábeas data (rotulado curiosamente en la misma ley con un alias: "acción de protección de los datos personales o habeas data") fue regulado expresamente en el último capítulo de la ley de protección de datos personales, pero sólo para los casos a ser tramitados ante la justicia federal, funcionando en concreto en los casos previstos en el art. 36 de la ley 25.326[23], es decir, cuando la acción se interponga

---

[21] La actividad del órgano de control ha sido sumamente importante desde el punto de vista institucional. A guisa de ejemplo valga recordar que durante el primer año de su gestión, el órgano de control desplegó múltiples actividades, pese a las dificultades de orden operativo que tuvo que afrontar. Según informes de su Director: a) se estableció un régimen de infracciones y sanciones, aplicable a quienes no cumplan con los preceptos de la ley 25.326 y su decreto reglamentario (disposición 1/2003); b) se aprobó el sistema de Registro de bases de datos privadas y se fijaron las modalidades del censo a producirse sobre todas las bases de datos alcanzadas por la ley (disposiciones 2/2003 y 1/2004); c) se aprobó el Reglamento Interno para el funcionamiento del Consejo Consultivo; d) se logró la calificación para la argentina de nivel adecuado de protección por la Unión Europea (decisión 2003/490/CE); e) se adhirió a la Red Iberoamericana de Protección de Datos, lanzada en el Seminario Internacional sobre Protección de Datos celebrada de Antigua, Guatemala; f) se diseñó una plataforma técnica de operación de la Red argentina de protección de los datos personales, para comenzar a consensuar los aspectos formales del Convenio de Ingreso de cada provincia en ella; g) se creó una página web (www.jus.gov.ar/minjus/dpdp) que facilita las consultas; h) se elaboraron formularios tipo para ejercer los derechos de acceso, rectificación, actualización y supresión de datos personales; i) se elaboraron proyectos de guías de aplicación práctica para los ámbitos financiero y de la salud, que se han elevado a los responsables de cada área; j) se realizaron las primeras coordinaciones a fin de fijar los estándares de protección de datos en el ámbito financiero conjuntamente con el Banco Central, ABA, ABAPRA, ADEBA y ABE; k) se comenzaron a analizar los Códigos de Conducta que se presentaron en diversas actividades de acuerdo a lo establecido por el art. 30 de la ley 25.326, para el posterior dictamen del Consejo Consultivo; l) se incoaron denuncias penales por violación a las disposiciones de la ley 25.326 (entre las que se destaca la formulada ante la Justicia Federal para investigar la presunta comisión de delitos contemplados en el art. 157 *bis* del Código Penal, por una supuesta transferencia internacional de datos de ciudadanos argentinos al gobierno de los Estados Unidos, efectuada por la firma *Choicepoint*; ll) se inició el análisis de los requisitos mínimos que se exigirán para considerar adecuado el nivel de protección proporcionado por las normas de un Estado u organismo internacional, a fin de autorizar transferencias internacionales; m) se estableció el Registro de sentencias relacionadas con el habeas data, en virtud de lo dispuesto por el art. 43, ap. 4, de la ley; n) se atendieron unas quinientas denuncias, quejas y reclamos; ñ) se elaboraron dictámenes, sobre diversos temas; o) se elaboraron manuales de protección de los datos, en especial respecto de los sensibles y de los bancarios respecto de informes crediticios, en tren de promover y difundir la cultura de protección de datos personales; p) se elaboraron criterios para establecer estándares específicos de protección de datos genéticos, de los niños y de los estudiantes universitarios; q) se elaboraron bases para convenios tipo de colaboración con las universidades; r) se colabora en la respectiva comisión del Ministerio del Interior para la base de datos de los DNI; s) se entablaron lazos con las agencias de protección de datos del Reino Unido, España, Francia, Canadá y Alemania; t) se llevaron a cabo varios seminarios y congresos con especialistas argentinos y extranjeros, y u) se iniciaron los trámites a fin de acreditar a la Dirección Nacional de Protección de Datos Personales como autoridad de protección de datos independiente en el marco de la Resolución adoptada por la 23º Conferencia Internacional de Comisionados para la Protección de Datos.

[22] CSJN, 15/10/98, Fallos…, 321:2767

[23] "Art. 36. – (Competencia). Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

"Procederá la competencia federal: a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y b) cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales."

contra organismos nacionales, y cuando los sistemas de información que contengan los datos se encuentren interconectados en redes nacionales o internacionales.

Los arts. 33 a 43 de la ley federal se ocupan concretamente de la acción y de su despliegue procesal (procedencia, legitimación activa y pasiva, competencia, procedimiento aplicable, requisitos de la demanda, trámite, contestación del informe, ampliación de la demanda y sentencia), pero no abordan todos los aspectos relacionados con el proceso de protección de los datos personales, pues sus disposiciones deben integrarse con las de otros tramos de la ley, del Código Procesal Civil y Comercial de la Nación y de la ley de amparo[24].

En concreto, las disposiciones del primer tramo de la ley que enuncian expresamente los supuestos que habilitan la acción de hábeas data, son el art. 14 (referente al derecho de acceso, al plazo concedido al legitimado pasivo para satisfacerlo y a la viabilización de la acción si no se da pleno cumplimiento a ese derecho dentro del plazo estipulado) y el art. 16 (que trata los derechos de rectificación, actualización y supresión de los datos, el plazo para que el sujeto pasivo cumpla con los requerimientos respectivos y la viabilización de la acción si éstos no son satisfechos).

La principal crítica que *prima facie* puede hacerse a estos artículos consiste en que las hipótesis previstas para que quede expedita la acción de hábeas data son francamente insuficientes, pues no sólo no se prevén todos los tipos constitucionalmente admitidos (p.ej., informativo autoral), sino que tampoco se contemplan otros propiciados por la doctrina y la jurisprudencia y que incluso surgen de las facultades reconocidas por la propia ley a los titulares de los datos (p.ej., inclusorio, disociador).

El diseño procesal escogido por el Senado –cámara de origen en el proyecto- se reformuló en la Cámara de Diputados, previéndose tres acciones especiales de hábeas data: a) de conocimiento; b) de prevención, y c) de reparación (esta última se concatenaba con una disposición específica -art. 46 en el proyecto- que partía de la presunción del daño infligido). Las originales previsiones introducidas por la Cámara de Diputados no fueron aceptadas por los senadores cuando el proyecto volviera a su consideración, quienes insistieron en la idea previa, pese a que no faltaron críticas acendradas al proyecto.

En efecto, el senador Rodríguez Saá propuso dejar de lado el proyecto y hacer uno más garantista, al estilo del propuesto por la Cámara de Diputados, que previera un proceso más corto, la competencia provincial y posibilidad de reclamar en ese proceso los daños y perjuicios sufridos[25]. Sin embargo, el criterio que finalmente imperó fue el del senador Menem, quien sostuvo que no tenía sentido distinguir en tres hábeas data distintos, si la acción es una sola, justificando su posición por cuanto "muchas veces se pierden juicios por no elegir bien cuál es la acción. Si bien se dice que pueden ser acumuladas, yo digo para qué determinar qué tipo de acción, complicando la ley. La acción es una sola, así como lo es el amparo. ¿O alguien ha visto que hay amparo para la restricción de derecho y otro para la violación de derecho? No, hay una sola acción"[26].

Las dos principales novedades que se introdujeron respecto de la acción de amparo fueron: a) la posibilidad de desdoblamiento del trámite, en una fase inicial, para acceder a los datos objeto de tratamiento y en una segunda fase, para operar sobre ellos, para lo cual debe ampliarse la demanda, y b) la regulación de cautelares específicas (en concreto, la anotación de controversia y el bloqueo de los datos cuestionados)[27].

---

[24] Así, por ejemplo, las reglas establecidas en este capítulo no son las únicas que se refieren de manera específica a los casos y condiciones de admisibilidad y procedencia de la acción, pues éstas pueden encontrarse tanto en los cuatro primeros capítulos, dedicados a los principios generales y a los derechos que reconoce la ley, como en los tres últimos, relativos al control administrativo y judicial y a las sanciones penales y administrativas por violaciones a esta norma. Desde luego, sólo en este segundo sector, y más precisamente en el último capítulo, se regula todo lo concerniente al trámite de la acción de hábeas data, para los casos que tramiten ante la justicia federal.

[25] "Antecedentes Parlamentarios", 2001–A–470 a 473.

[26] "Antecedentes Parlamentarios", 2001–A–476 y 477.

[27] "Art. 38.– (Requisitos de la demanda). …3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial.

"4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate."

"Art. 39.– (Trámite). 1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente. 2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez.

"Art. 41.– Contestación del informe). Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley."

"Art. 42.– (Ampliación de la demanda). Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días."

En el plano de los estados federados, la mayoría reformó sus constituciones e incorporó a la acción de hábeas data[28], pero muy pocos dictaron normas específicas tendientes a regular su trámite procesal -en concreto, las provincias de Chubut (ley n° 4244, de 1996); Chaco (ley n° 4360, de 1996); Río Negro (ley n° 3246, de 1998); San Juan (ley n° 7447, de 2004), y Ciudad Autónoma de Buenos Aires (ley n° 1845 de 2005)-, pese a que a partir de las pautas competenciales emergentes del art. 36 de la ley 25.326 queda claro que también debe regularse adecuadamente el proceso de hábeas data en los ámbitos locales.

Hasta el momento este proceso es demasiado lento, pese al prudencial tiempo transcurrido desde la aprobación de la ley n° 25.326, por lo que la deuda de los estados federados debiera ser saldada a la brevedad a fin de brindar correcta tutela al derecho a la protección de datos en toda la República.

3. BALANCE CONCLUSIVO Y PROPUESTAS

[28] *Ciudad Autónoma de Buenos Aires*: "Art. 16.– Toda persona tiene, mediante una acción de amparo, libre acceso a todo registro, archivo o banco de datos que conste en organismos públicos o en los privados destinados a proveer informes, a fin de conocer cualquier asiento sobre su persona, su fuente, origen, finalidad o uso que del mismo se haga.

"También puede requerir su actualización, rectificación, confidencialidad o supresión, cuando esa información lesione o restrinja algún derecho.

"El ejercicio de este derecho no afecta el secreto de la fuente de información periodística."

Provincia de Buenos Aires: "Art. 20.– Se establecen las siguientes garantías de los derechos constitucionales: [...] 3. A través de la garantía de hábeas data, que se regirá por el procedimiento que la ley determine, toda persona podrá conocer lo que conste de la misma en forma de registro, archivo o bancos de datos de organismos públicos, o privados destinados a proveer informes, así como la finalidad a que se destine esa información, y a requerir su rectificación, actualización o cancelación. No podrá afectarse el secreto de las fuentes y el contenido de la información periodística.

"Ningún dato podrá registrarse con fines discriminatorios ni será proporcionado a terceros, salvo que tengan un interés legítimo. El uso de la informática no podrá vulnerar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos."

Córdoba: "Art. 50.– Toda persona tiene derecho a conocer lo que de ella conste en forma de registro, la finalidad a que se destine esa información, y a exigir su rectificación y actualización. Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando tengan un interés legítimo. La ley reglamenta el uso de la informática para que no se vulneren el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos".

Chaco: "Art. 19 [...] Toda persona tiene derecho a informarse de los datos que sobre sí mismo, o sobre sus bienes, obren en forma de registros o sistemas oficiales o privados de carácter público; la finalidad a que se destine esa información, y a exigir su actualización, corrección, supresión o confidencialidad.

"Tales datos no podrán ser utilizados con fines discriminatorios de ninguna especie.

"No podrá afectarse el secreto de las fuentes de información periodística [...]".

Chubut: "Art. 56.– Toda persona puede interponer acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o en los privados destinados a proveer informes, y en caso de error, omisión, falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No puede afectarse el secreto de la fuente de información periodística."

Jujuy: "Art. 23.– [...] 6) Todas las personas tienen derecho de tomar conocimiento de lo que constare a su respecto en los registros provinciales de antecedentes personales y del destino de esas informaciones, pudiendo exigir la rectificación de los datos. Queda prohibido el acceso a terceros a esos registros, así como su comunicación o difusión, salvo en los casos expresamente previstos por la ley. [...] 8) El procesamiento de datos por cualquier medio o forma nunca puede ser utilizado para su registro y tratamiento con referencia a convicciones filosóficas, ideológicas o políticas, filiación partidaria o sindical, creencias religiosas o respecto de la vida privada, salvo que se tratare de casos no individualmente identificables y para fines estadísticos".

La Rioja: "Art. 30.– …La ley limitará el uso de la informática para preservar el honor, la intimidad personal y familiar de los habitantes y el pleno ejercicio de sus derechos… Las autoridades policiales sólo proporcionarán antecedentes penales de los habitantes en los casos previstos por la ley".

Río Negro: "Art. 20.– La ley asegura la intimidad de las personas. El uso de información de toda índole o categoría, almacenada, procesada o distribuida por cualquier medio físico o electrónico, debe respetar el honor, la privacidad y el goce completo de los derechos. La ley reglamenta su utilización de acuerdo a los principios de justificación social, limitación de la recolección de datos, calidad, especificación del propósito, confidencialidad, salvaguardia de la seguridad, apertura de los registros, limitación en el tiempo y control público. Asegura el acceso de las personas afectadas a la información para su rectificación, actualización o cancelación cuando no fuera razonable su mantenimiento".

Salta: "Art. 22.– [...] Las autoridades policiales proporcionan antecedentes penales o judiciales de los habitantes exclusivamente en los casos previstos por la ley".

San Juan: "Art. 26.– Todo ciudadano tiene derecho a tomar conocimiento de lo que de él conste en forma de registro y de la finalidad a que se destinan las informaciones, pudiendo exigir la rectificación de datos, así como su actualización. No se puede utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se destine para fines estadísticos no identificables".

"Art. 27.– Todos los habitantes tienen derecho a que se les informe veraz y auténticamente sin distorsiones de ningún tipo, teniendo también el derecho al libre acceso a las fuentes de información, salvo en asuntos vitales para la seguridad del Estado. El tiempo de la reserva se fijará por ley. Los registros de antecedentes personales harán figurar en las certificaciones que emitan solamente las causas con condenas no cumplidas contra el interesado, salvo solicitud de autoridad judicial o del mismo interesado. No hay restricción alguna para introducir publicaciones, distribuírlas en el interior de la Provincia, programar, organizar y asistir a congresos de carácter provincial, nacional o internacional. La información en todos sus aspectos es considerada como de interés público".

San Luis: "Art. 21.– [...] Todos los habitantes de la Provincia tienen derecho a tomar conocimiento de lo que de ellos conste en registros de antecedentes personales e informarse sobre la finalidad a que se destinan dichos registros y la fuente de información en que se obtienen los datos respectivos".

Tierra del Fuego: "Art. 45.– Toda persona tiene derecho a conocer lo que de ella conste en forma de registro y la finalidad a que se destine esa información, y a exigir su rectificación y actualización. Esos datos no pueden registrarse con propósitos discriminatorios de ninguna clase, ni ser proporcionados a terceros, excepto cuando éstos tengan un interés legítimo".

De todo lo expuesto es fácil colegir que Iberoamérica está transitando, cada vez con más velocidad pero sin vértigo, el camino hacia normativas comunes que puedan homogeneizar de algún modo el tratamiento de los datos personales en la región.

Los problemas más cruciales son, evidentemente, los relacionados con la localización de la autoridad de control y la extensión de sus facultades, donde se nota una gran renuencia en toda América Latina a establecer órganos jerárquicamente independientes del poder ejecutivo, que es quien tiene la inmensa mayoría de las bases de datos que estos órganos deben controlar.

La ausencia o falta de poderes efectivos del órgano de control ha provocado que la tutela efectiva del derecho se encontrara en las vías judiciales, especialmente a través del proceso de hábeas data, y de manera individual –aunque en algunos casos se han admitido hábeas datas de tipo colectivo, frente a violaciones generalizadas que podrían causar discriminación-.

Esta acción y el proceso constitucional consecuente en la mayoría de los casos ha suplido y en otros –unos pocos- ha coadyuvado en la labor de control administrativo, que como ya dijimos, puede o no existir, de acuerdo al país de que se trate.

Sin embargo, es necesario redimensionar el control en su justo cauce: existiendo posibilidades de ejercer un control homogéneo y concentrado en esta materia, que es hoy por hoy una disciplina de “alta complejidad”, a punto tal que se ha convertido en un típico “microsistema” que no todos los operadores del derecho comprenden acabadamente, resulta poco razonable que predomine el control judicial sobre el administrativo, por lo que se impone realizar y aún profundizar los cambios propiciados por el Grupo de Trabajo del art. 29 de la Directiva Europea 95/46. Otros problemas que se han ido sumando gradualmente a los iniciales (v.gr., los problemas relacionados con la videovigilancia, el “spam telefónico”, las redes sociales, entre muchos otros), coadyuvan a que se reclame una solución inteligente e integral a los problemas.

Al fragor de estas nuevas problemáticas seguramente surgirán los cambios. Los que vienen serán tiempos promisorios, y deben ser transitados sin pausa, buscando que en definitiva se dé efectiva vigencia al derecho a la protección de datos.